PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-134534

(43)Date of publication of application : 18.05.2001

(51)Int.Cl. G06F 15/00
G06F 13/00

(21)Application number : 11-317468

(22)Date of filing : 08.11.1999

(71)Applicant : NTT COMMUNICATIONS KK

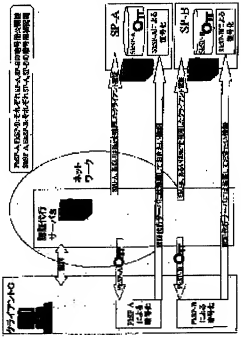
(72)Inventor : HIKITA TOMOHARU
YASUDA HITOSHI
YAMAMOTO MORITAKA
KUWATA MASAHIKO
IMAIZUMI NORIKO
SHIMAZAKI TAKESHI

(54) AUTHENTICATION DELEGATE METHOD, AUTHENTICATION DELEGATE SERVICE SYSTEM, AUTHENTICATION DELEGATE SERVER DEVICE, AND CLIENT DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent information from leaking to an authentication delegate server which acts for authentication.

SOLUTION: The authentication delegate server S distributes an open key for ciphering of service providers SP-A and SP-B made to correspond to desirable service to a client C and transfers ciphered information received from the client C to the providers SP-A and SP-B when the service is provided. The client C ciphers the information to be sent to the providers SP-A and SP-B by using the open key for ciphering received from an authentication delegate server S and sends the ciphered information to the authentication delegate server S. The providers SP-A and SP-B decipher the ciphered information received from the authentication delegate server S by using a secret key for ciphering.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] In the authentication vicarious execution approach that the authentication vicarious execution server equipment formed between the service provider equipment which offers service, and the client equipment which receives service provision receives authentication from said service provider equipment instead of said client equipment At the time of service provision The procedure which delivers the public key for codes of said service provider equipment corresponding to desired service from said authentication vicarious execution server equipment to said client equipment, The procedure of enciphering using the public key for codes which received the information which should be transmitted to said service provider equipment in said client equipment from said authentication vicarious execution server equipment, and transmitting this enciphered information to said authentication vicarious execution server equipment, The procedure of transmitting the enciphered information which was received from said client equipment to said service provider equipment from said authentication vicarious execution server equipment, It has the procedure which decrypts the enciphered information which was received from said authentication vicarious execution server equipment in said service provider equipment using the private key for codes. The authentication vicarious execution approach characterized by performing information transfer from client equipment to service provider equipment, without revealing to authentication vicarious execution server equipment.
[Claim 2] In the authentication vicarious execution approach that the authentication vicarious execution server equipment formed between the service provider equipment which offers service, and the client equipment which receives service provision receives authentication from said service provider equipment instead of said client equipment At the time of service provision The procedure which delivers the public key for codes of said client equipment from said authentication vicarious execution server equipment to said service provider equipment corresponding to desired service, The procedure of enciphering using the public key for codes which received the information which should be transmitted to said client equipment in said service provider equipment from said authentication vicarious execution server equipment, and transmitting this enciphered information to said authentication vicarious execution server equipment, The procedure of transmitting the enciphered information which was received from said service provider equipment to said client equipment from said authentication vicarious execution server equipment, It has the procedure which decrypts the enciphered information which was received from said authentication vicarious execution server equipment in said client equipment using the private key for codes. The authentication vicarious execution

approach characterized by performing information transfer from service provider equipment to client equipment, without revealing to authentication vicarious execution server equipment.

[Claim 3] In the authentication vicarious execution approach that the authentication vicarious execution server equipment formed between the service provider equipment which offers service, and the client equipment which receives service provision receives authentication from said service provider equipment instead of said client equipment At the time of service provision The procedure which delivers the public key for codes of said service provider equipment corresponding to desired service from said authentication vicarious execution server equipment to said client equipment, The data which become in said client equipment the session key for cryptocommunication between said service provider equipment or the origin of this session key are generated. The procedure of enciphering using the public key for codes which received said session key or data from said authentication vicarious execution server equipment, and transmitting this enciphered information to said authentication vicarious execution server equipment, The procedure of transmitting the enciphered information which was received from said client equipment to said service provider equipment from said authentication vicarious execution server equipment, Decrypt the enciphered information which was received from said authentication vicarious execution server equipment in said service provider equipment using the private key for codes, and said session key is acquired. Or said data are acquired by the decryption using the private key for codes. The procedure which generates said session key, and the information which should be transmitted in said client equipment or said service provider equipment are enciphered using said session key from this data. The procedure of transmitting this enciphered information to said authentication vicarious execution server equipment, The procedure of transmitting the information enciphered using said session key from said authentication vicarious execution server equipment to said service provider equipment or said client equipment, It has the procedure decrypted using said session key to which self has the information enciphered using said session key in said service provider equipment or said client equipment. The authentication vicarious execution approach characterized by performing bidirectional information transfer between client equipment and service provider equipment, without revealing to authentication vicarious execution server equipment.

[Claim 4] The procedure which delivers the public key certificate for codes with said public key for codes in the authentication vicarious execution approach according to claim 1 or 3 in case said public key for codes is delivered from said authentication vicarious execution server equipment to said client equipment, The authentication vicarious execution approach characterized by having the procedure of verifying said public key for codes based on the public key certificate for codes received from said authentication vicarious execution server equipment before performing encryption using said public key for codes in said client equipment.

[Claim 5] In the authentication vicarious execution approach according to claim 1 or 3, in case it enciphers in said client equipment The procedure of enciphering the authentication information on this client equipment using said public key for codes, and transmitting this enciphered information to said authentication vicarious execution server equipment, In case it decrypts in said service provider equipment, decrypt the enciphered information which was received from said authentication vicarious execution server equipment using

the private key for codes, and said authentication information is acquired. The authentication vicarious execution approach characterized by having the procedure which attests said client equipment based on this authentication information.
[Claim 6] The service provider equipment which offers service, and the client equipment which was connected with said service provider equipment and which receives service provision, It consists of authentication vicarious execution server equipment formed between said service provider equipment and client equipment. In the authentication vicarious execution service system with which said authentication vicarious execution server equipment receives authentication from said service provider equipment instead of said client equipment said authentication vicarious execution server equipment The public key for codes of said service provider equipment corresponding to desired service is delivered to said client equipment at the time of service provision. It has a means to transmit the enciphered information which was received from said client equipment to said service provider equipment. Said client equipment It enciphers using the public key for codes which received the information which should be transmitted to said service provider equipment from said authentication vicarious execution server equipment. It has a means to transmit this enciphered information to said authentication vicarious execution server equipment. Said service provider equipment The authentication vicarious execution service system characterized by performing information transfer from client equipment to service provider equipment, without having a means to decrypt the enciphered information which was received from said authentication vicarious execution server equipment using the private key for codes, and revealing to authentication vicarious execution server equipment.
[Claim 7] The service provider equipment which offers service, and the client equipment which was connected with said service provider equipment and which receives service provision, It consists of authentication vicarious execution server equipment formed between said service provider equipment and client equipment. In the authentication vicarious execution service system with which said authentication vicarious execution server equipment receives authentication from said service provider equipment instead of said client equipment said authentication vicarious execution server equipment As opposed to said service provider equipment corresponding to desired service the time of service provision Deliver the public key for codes of said client equipment, and it has a means to transmit the enciphered information which was received from said service provider equipment to said client equipment. Said service provider equipment is enciphered using the public key for codes which received the information which should be transmitted to said client equipment from said authentication vicarious execution server equipment. It has a means to transmit this enciphered information to said authentication vicarious execution server equipment. Said client equipment The authentication vicarious execution service system characterized by performing information transfer from service provider equipment to client equipment, without having a means to decrypt the enciphered information which was received from said authentication vicarious execution server equipment using the private key for codes, and revealing to authentication vicarious execution server equipment.
[Claim 8] The service provider equipment which offers service, and the client equipment which was connected with said service provider equipment and which receives service provision, It consists of authentication vicarious execution server equipment formed

between said service provider equipment and client equipment. In the authentication vicarious execution service system with which said authentication vicarious execution server equipment receives authentication from said service provider equipment instead of said client equipment said authentication vicarious execution server equipment The public key for codes of said service provider equipment corresponding to desired service is delivered to said client equipment at the time of service provision. The enciphered information which was received from said client equipment is transmitted to said service provider equipment. It has a means to transmit the enciphered information which was received from said service provider equipment to said client equipment. Said client equipment The data which become the session key for cryptocommunication between said service provider equipment or the origin of this session key are generated. It enciphers using the public key for codes which received said session key or data from said authentication vicarious execution server equipment. After transmitting this enciphered information to said authentication vicarious execution server equipment, the information which should be transmitted to said service provider equipment is enciphered using said session key. It has a means to transmit this enciphered information to said authentication vicarious execution server equipment. Said service provider equipment Decrypt the enciphered information which was received from said authentication vicarious execution server equipment using the private key for codes, and acquire said session key, or said data are acquired by the decryption using the private key for codes. After generating said session key from this data, the information which should be transmitted to said client equipment is enciphered using said session key. The authentication vicarious execution service system characterized by performing bidirectional information transfer between client equipment and service provider equipment, without having a means to transmit this enciphered information to said authentication vicarious execution server equipment, and revealing to authentication vicarious execution server equipment.

[Claim 9] In an authentication vicarious execution service system according to claim 6 or 8 said authentication vicarious execution server equipment In case said public key for codes is delivered to said client equipment, it has a means to deliver the public key certificate for codes with said public key for codes. Said client equipment The authentication vicarious execution service system characterized by having a means to verify said public key for codes based on the public key certificate for codes received from said authentication vicarious execution server equipment before performing encryption using said public key for codes.

[Claim 10] In an authentication vicarious execution service system according to claim 6 or 8 said client equipment In case said encryption is performed, use said public key for codes and the authentication information on self-equipment is enciphered. It has a means to transmit this enciphered information to said authentication vicarious execution server equipment. Said service provider equipment The authentication vicarious execution service system characterized by having the means which decrypts the enciphered information which was received from said authentication vicarious execution server equipment using the private key for codes, acquires said authentication information, and attests said client equipment based on this authentication information in case said decryption is performed.

[Claim 11] In the authentication vicarious execution server equipment which is formed

between the service provider equipment which offers service, and the client equipment which receives service provision, and receives authentication from said service provider equipment instead of said client equipment Said authentication vicarious execution server equipment delivers the public key for codes of said service provider equipment corresponding to desired service to said client equipment at the time of service provision. Authentication vicarious execution server equipment characterized by having a means to transmit said enciphered information to said service provider equipment in order to make the decryption using the reception from said client equipment, and the private key for codes of the information enciphered using this public key for codes perform.

[Claim 12] In the authentication vicarious execution server equipment which is formed between the service provider equipment which offers service, and the client equipment which receives service provision, and receives authentication from said service provider equipment instead of said client equipment As opposed to said service provider equipment corresponding to [the time of service provision] desired service in said authentication vicarious execution server equipment The information which delivered the public key for codes of said client equipment, and was enciphered using this public key for codes From said service provider equipment to reception Authentication vicarious execution server equipment characterized by having a means to transmit said enciphered information to said client equipment in order to make the decryption using the private key for codes perform.

[Claim 13] In the authentication vicarious execution server equipment which is formed between the service provider equipment which offers service, and the client equipment which receives service provision, and receives authentication from said service provider equipment instead of said client equipment Said authentication vicarious execution server equipment delivers the public key for codes of said service provider equipment corresponding to desired service to said client equipment at the time of service provision. The data which become the session key for cryptocommunication enciphered using this public key for codes, or the origin of this session key From said client equipment to reception After transmitting said enciphered session key or data to said service provider equipment in order to make the decryption using the private key for codes perform, While transmitting the information from said client equipment enciphered using said session key to said service provider equipment Authentication vicarious execution server equipment characterized by having a means to transmit the information from said service provider equipment enciphered using said session key to said client equipment.

[Claim 14] It is authentication vicarious execution server equipment characterized by having a means to deliver the public key certificate for codes to said client equipment with said public key for codes so that said authentication vicarious execution server equipment may make said public key for codes verify to said client equipment in authentication vicarious execution server equipment according to claim 11 or 13.

[Claim 15] Between the service provider equipment which offers service, and the client equipment which receives service provision It is said client equipment in the authentication vicarious execution service system with which the formed authentication vicarious execution server equipment receives authentication from said service provider equipment instead of said client equipment. While consisting of an IC card equipped with a signature generation means to generate the signature for receiving client authentication from said authentication vicarious execution server equipment An encryption means to

encipher the information which should be transmitted to said service provider equipment using the public key for codes, The signature generated with said IC card is transmitted to said authentication vicarious execution server equipment. Client equipment characterized by consisting of a processor equipped with a transceiver means to transmit the information which received the public key for codes transmitted from said authentication vicarious execution server equipment, outputted to said encryption means, and was enciphered by said encryption means to said authentication vicarious execution server equipment.

[Claim 16] Between the service provider equipment which offers service, and the client equipment which receives service provision It is said client equipment in the authentication vicarious execution service system with which the formed authentication vicarious execution server equipment receives authentication from said service provider equipment instead of said client equipment. A signature generation means to generate the signature for receiving client authentication from said authentication vicarious execution server equipment, While consisting of an IC card equipped with an encryption means to encipher the information which should be transmitted to said service provider equipment using the public key for codes The signature generated with said IC card is transmitted to said authentication vicarious execution server equipment. Client equipment characterized by consisting of a processor equipped with a transceiver means to transmit the information which received the public key for codes transmitted from said authentication vicarious execution server equipment, outputted to said IC card, and was enciphered with said IC card to said authentication vicarious execution server equipment.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the authentication vicarious execution approach that the authentication vicarious execution server equipment formed between service provider equipment and client equipment receives authentication from service provider equipment instead of client equipment, an authentication vicarious execution service system, authentication vicarious execution server equipment, and client equipment.

[0002]

[Description of the Prior Art] Conventionally, generally in the service provision by the network, performing client authentication using confidential information is performed. Here, confidential information points out the share key of share key methods, such as a private key in public key cryptosystems, such as a password and RSA (Rivest and Shamir and Adleman), and DES (Data Encryption Standard). When performing client authentication, generally to a different service provider, that from which confidential information differs is used.

[0003] For example, as shown in drawing 13 , in case a certain client equipment (it abbreviates to a client hereafter) C accesses the service A offered by service provider equipment (it abbreviates to service provider hereafter) SP-A, and the service B offered by service provider SP-B, respectively, it is necessary to receive client authentication using respectively different confidential information SkU-A and respectively different

SkU-B. In drawing 13 , CertU-A and CertU-B are the certificates corresponding to confidential information SkU-A and SkU-B, respectively. This certificate is unnecessary depending on a method. For example, in a public key cryptosystem, confidential information SkU serves as a private key, and CertU serves as a public key certificate. In addition, a "service provider" here does not necessarily mean the service provider (for example, company) in the actual world. That is, even if the service provider in the actual world is the same, the case "where service providers differ" is possible. For example, inquiry-for-the-balances service of a certain bank and investment fund application service are considered to be the services offered by another service provider.

[0004] If it agrees with sharing of client information between different service providers, it is possible to make confidential information the same. For example, if it says in the example shown in drawing 13 and service provider SP-A and SP-B will agree, it is possible to receive offer of Service B using confidential information SkU-A to service provider SP-A (drawing 14). Especially, if it is two services of the same bank in the above-mentioned example, since service provider SP-A and SP-B are the same, agreement is comparatively easy in the actual world. However, it is difficult to agree among all the existing service providers, and it is not realistic. Many cases where agreement is difficult exist in Client C by the difference in the plan at the time of publishing confidential information, the difference in the reinforcement of confidential information, the difference in the demand security of service, etc. That is, since the plans of each service provider about client authentication differ, many cases where agreement is difficult exist.

[0005] When the plan about client authentication is in agreement to some extent, it may be possible by constituting a certificate authority hierarchical to receive authentication by the same confidential information. For example, as shown in drawing 15 , an authentication tree consists of forms where certificate authority CA-A or CA-B publishes the certificate to confidential information, and certificate authority CA-R of a high order publishes a certificate further to the confidential information of the certificate authority CA-A and CA-B. And if the authentication tree to the confidential information of service provider SP-A and the authentication tree to the confidential information of service provider SP-B have an intersection in the high order, service provider SP-B may be able to offer service by confidential information SkU-A. In drawing 15 , a certificate authority for CA-A and CA-B to receive service of service provider SP-A and CA-R are the certificate authorities of the high order of certificate authority CA-A and CA-B. In addition, other certificate authorities may be placed between the middle of CA-A, CA-B, and CA-R, or the high order of CA-R. Service provider SP-B accepts the client authentication using confidential information SkU-A with the certificate which CA-A which high order certificate authority CA-R of CA-B which is the certificate authority of a self-client has attested published.

[0006] In the case of drawing 15 , it is difficult to give an intersection to the authentication tree of all services, and even if there is an intersection, service provision is not necessarily possible by the difference in the plan of security etc. That is, even if it realizes who Client C is, service provision can be refused depending on the plan of a service provider. Therefore, generally "when receiving two or more services which need client authentication, a client needs to manage two or more confidential information corresponding to each service" can say. Here, suppose that the case where the same

confidential information can receive authentication is called "the same [the authentication system of service]." Suppose that the case where the same confidential information cannot receive authentication on the contrary is called saying "The authentication systems of service differ."

[0007] The cost which generally mounts the function manager of confidential information and the function to receive client authentication using confidential information in Client C becomes still larger [it is large, and], when using two or more confidential information to two or more services. Since there is risk of other clients turning into a self-client and clearing up when the problem of it becoming impossible to receive service arises when confidential information is lost, and confidential information is revealed if it says about management of confidential information, the cost of mounting of a loss prevention function and a leakage control function becomes large. When two or more confidential information needs to be managed, the cost of the management [itself] becomes large, up, if some one confidential information is lost and revealed depending on a management gestalt, the recurrence line of other confidential information may have to be carried out, and recurrence line cost will turn large.

[0008] When using a public key cryptosystem about the client authentication function using confidential information, for example, the storage function of a public key certificate [/ in addition to management of a private key], the transmitting function to the service provider of a public key certificate, the generation function of confidential information (key pair in a public key cryptosystem etc.), the add function of the confidential information to a certificate authority, a public key certification dictation profit function, etc. are needed for Client C. When a simple terminal, for example, a set top box etc., is assumed to Client C, even if there is little confidential information to manage, the cost which mounts all these functions is large, but it will become still larger if confidential information increases. From such a thing, a demand of the client manager who wants to lessen the number of the confidential information managed by Client C as much as possible exists.

[0009] When receiving a demand of such a client manager, i.e., two or more services from which an authentication system differs, there are the following three as a conventional technique which solves wanting to lessen confidential information which a client manager manages.

Conventional technique 1: Mutual recognition of certificate authorities.

Conventional technique 2: Commission of authentication processing with the gestalt which deposits authentication vicarious execution SABAHE confidential information.

Conventional technique 3: Commission of authentication processing with the gestalt using own confidential information of an authentication vicarious execution server.

[0010] As shown in drawing 16 , when it does not have an intersection in an authentication tree, or when [though it has the conventional technique 1,] its plan about each SP's authentication does not correspond on the level in which the service provision concerned is possible, it is a method which enables it to receive authentication by the same confidential information by checking the mutual recognition document of certificate authority CA-A0 and CA-B0 comrades. In drawing 16 , CA-A1, CA-A2, CA-B1, and CA-B-2 are [certificate authority CA-A1, the certificate authority of the high order of CA-A2 and CA-B0 of a certificate authority and CA-A0] the certificate authorities of the high order of certificate authority CA-B1 and CA-B-2. Service provider SP-B accepts the

client authentication using confidential information SkU-A, when a mutual recognition document exists between high order certificate authority CA-B0 of the certificate authority (for example, CA-B1) of a self-client, and other high order certificate authority CA-A0. This conventional technique 1 is one of the promising methods. However, since a big functional addition being required for a service provider or a certificate authority, and publishing a mutual recognition document needs agreement formation of each service provider after all, applicability is restricted. Therefore, in this invention, it does not consider as the object of consideration.

[0011] The conventional technique 2 is a method which forms the authentication vicarious execution server S which manages the confidential information in other authentication systems, a certificate, CRL (lapse certificate list), etc. in one authentication system to which Client C belongs, and attests about the service which needs client authentication between the authentication vicarious execution server S, each service provider SP-A, and SP-B, as shown in drawing 17 . In drawing 17 , SkU-P is the confidential information for using for authentication between the authentication vicarious execution server S and Client C. About this confidential information SkU-P, a client manager may memorize and it may not manage by client C itself. Moreover, CertU-P is a certificate corresponding to confidential information SkU-P. This certificate is unnecessary depending on a method. For example, in a public key cryptosystem, confidential information SkU-P serves as a private key, and CertU-P serves as a public key certificate.

[0012] The conventional technique 2 has the advantage that there is little modification in a certificate authority and service provider side compared with the conventional technique 1. If it sees from a certificate authority and service provider side, he will not be conscious of the authentication vicarious execution server S, and it will be attested as a client C. For example, although it is necessary to hold confidential information, respectively in order user authentication is needed in SET (SecureElectronic Transaction) and SECE (Secure Electronic Commerce Environment) which are the method which realizes the credit settlement of accounts and bank account settlement of accounts on the Internet and to receive service from two or more credit firms and banks, the method which deposits this confidential information with the authentication vicarious execution server called Sir BAWO let is proposed, and the part is produced commercially.

[0013] As shown in drawing 18 , in case the conventional technique 3 receives client authentication from service provider SP-A and SP-B, the confidential information of each client C is a method using the own confidential information SkP of authentication vicarious execution server S rather than it is used for it. In drawing 18 , CertP is a certificate corresponding to confidential information SkP. That is, from a service provider side, it seems that the authentication vicarious execution server S has received service. With this conventional technique 3, like the conventional technique 2, each client C does not need to manage the confidential information corresponding to each service, and should manage only own confidential information also in the authentication vicarious execution server S.

[0014]

[Problem(s) to be Solved by the Invention] However, there were the three following troubles in the above conventional technique 2 and the conventional technique 3.

Trouble 1: All the information exchanged between Client C, service provider SP-A, and

SP-B is revealed to the authentication vicarious execution server S. Although the authentication vicarious execution server S is the subject who can trust it for Client C, there is a case where he wants to keep secret the information exchanged with service provider SP-A and SP-B depending on service. Temporarily, within the authentication vicarious execution server S, though between the authentication vicarious execution server S, service provider SP-A, and SP-B is enciphered, respectively, since information is decrypted, there is a possibility that information may be revealed between Client C and the authentication vicarious execution server S. In addition, this trouble 1 is common on both conventional technique 2 and conventional technique 3.

[0015] Trouble 2: When the authentication vicarious execution server S becomes Client C and clears up, it cannot check in a service provider SP-A and SP-B side. In the conventional technique 2, since the authentication vicarious execution server S holds client confidential information, it becomes Client C and it can be cleared up. As for the authentication vicarious execution server S, it is desirable to prepare the means which can attest a direct client by the service provider SP-A and SP-B side, for example, if the case where the systems operation person of the authentication vicarious execution server S etc. should commit injustice, the case where it is denied that the client user received offer of service, etc. are assumed although it is generally the subject who can trust it also from service provider SP-A and SP-B also from a user. Of course, considering the advantage of the authentication vicarious execution server S existing, the authentication means in that case needs to be simple compared with the case where the authentication vicarious execution server S does not exist.

[0016] Trouble 3: It is easy to produce the responsibility of offering service between Client C, service provider SP-A, and SP-B, and the responsibility of collecting service countervalues in the authentication vicarious execution server S. In the conventional technique 3, service provider SP-A and SP-B attest a client by own confidential information of authentication vicarious execution server S, and perform service provision. that is, service provider SP-A and SP-B offer service being conscious of the authentication vicarious execution server S, and it is easy to produce the responsibility of sending the service to Client C, and the responsibility of collecting a service countervalue from Client C in the authentication vicarious execution server S (a contract between persons concerned in whether it is actually generated, and law -- based on a system). In that case, the more responsibility becomes large, the more the subject who can manage the authentication vicarious execution server S will be restricted. It aims at offering the authentication vicarious execution approach which can cancel said trouble 1, a trouble 2, and a trouble 3, an authentication vicarious execution service system, authentication vicarious execution server equipment, and client equipment, solving [this invention was made in order to solve the above-mentioned technical problem, and] the burden of the client about authentication by the authentication vicarious execution server.

[0017]

[Means for Solving the Problem] As for the authentication vicarious execution approach of this invention, the authentication vicarious execution server equipment formed between the service provider equipment which offers service, and the client equipment which receives service provision receives authentication from service provider equipment instead of client equipment. And the procedure in which the authentication vicarious execution approach of this invention delivers the public key for codes of the service

provider equipment corresponding to desired service from authentication vicarious execution server equipment to client equipment at the time of service provision, The procedure of enciphering using the public key for codes which received the information which should be transmitted to service provider equipment in client equipment from authentication vicarious execution server equipment, and transmitting this enciphered information to authentication vicarious execution server equipment, The procedure of transmitting the enciphered information which was received from client equipment to service provider equipment from authentication vicarious execution server equipment, It has the procedure which decrypts the enciphered information which was received from authentication vicarious execution server equipment in service provider equipment using the private key for codes. Moreover, the authentication vicarious execution approach of this invention receives the service provider equipment corresponding to desired service at the time of service provision. The procedure which delivers the public key for codes of client equipment from authentication vicarious execution server equipment, The procedure of enciphering using the public key for codes which received the information which should be transmitted to client equipment in service provider equipment from authentication vicarious execution server equipment, and transmitting this enciphered information to authentication vicarious execution server equipment, It has the procedure of transmitting the enciphered information which was received from service provider equipment to client equipment from authentication vicarious execution server equipment, and the procedure which decrypts the enciphered information which received from authentication vicarious execution server equipment in client equipment using the private key for codes.

[0018] Moreover, the procedure in which the authentication vicarious execution approach of this invention delivers the public key for codes of the service provider equipment corresponding to desired service from authentication vicarious execution server equipment to client equipment at the time of service provision, The data which become in client equipment the session key for cryptocommunication between service provider equipment or the origin of this session key are generated. The procedure of enciphering using the public key for codes which received a session key or data from authentication vicarious execution server equipment, and transmitting this enciphered information to authentication vicarious execution server equipment, The procedure of transmitting the enciphered information which was received from client equipment to service provider equipment from authentication vicarious execution server equipment, Decrypt the enciphered information which was received from authentication vicarious execution server equipment in service provider equipment using the private key for codes, and acquire a session key, or data are acquired by the decryption using the private key for codes. The procedure which generates a session key, and the information which should be transmitted in client equipment or service provider equipment are enciphered using a session key from this data. The procedure of transmitting this enciphered information to authentication vicarious execution server equipment, and the procedure of transmitting the information enciphered using the session key from authentication vicarious execution server equipment to service provider equipment or client equipment, It has the procedure decrypted using the session key to which self has the information enciphered using the session key in service provider equipment or client equipment.

[0019] Moreover, as an example of 1 configuration of the authentication vicarious-

execution approach of this invention, in case the public key for codes is delivered from authentication vicarious-execution server equipment to client equipment, it has the procedure verify the public key for codes the procedure which delivers the public key certificate for codes with the public key for codes, and based on the public key certificate for codes received from authentication vicarious-execution server equipment before performing encryption using the public key for codes in client equipment. Moreover, in case it enciphers in client equipment as an example of 1 configuration of the authentication vicarious execution approach of this invention The procedure of enciphering the authentication information on this client equipment using the public key for codes, and transmitting this enciphered information to authentication vicarious execution server equipment, In case it decrypts in service provider equipment, the enciphered information which was received from authentication vicarious execution server equipment is decrypted using the private key for codes, authentication information is acquired, and it has the procedure which attests client equipment based on this authentication information.

[0020] As an authentication vicarious execution service system of this invention, moreover, authentication vicarious execution server equipment (S) The public key for codes of the service provider equipment corresponding to desired service is delivered to client equipment at the time of service provision. It has a means to transmit the enciphered information which was received from client equipment to service provider equipment. Client equipment (C) It enciphers using the public key for codes which received the information which should be transmitted to service provider equipment from authentication vicarious execution server equipment. Having a means to transmit this enciphered information to authentication vicarious execution server equipment, service provider equipment (SP-A, SP-B) has a means to decrypt the enciphered information which was received from authentication vicarious execution server equipment using the private key for codes. As an authentication vicarious execution service system of this invention, moreover, authentication vicarious execution server equipment (S) As opposed to the service provider equipment corresponding to desired service the time of service provision Deliver the public key for codes of client equipment, and it has a means to transmit the enciphered information which was received from service provider equipment to client equipment. Service provider equipment (SP-A, SP-B) It enciphers using the public key for codes which received the information which should be transmitted to client equipment from authentication vicarious execution server equipment. Having a means to transmit this enciphered information to authentication vicarious execution server equipment, client equipment (C) has a means to decrypt the enciphered information which was received from authentication vicarious execution server equipment using the private key for codes.

[0021] As an authentication vicarious execution service system of this invention, moreover, authentication vicarious execution server equipment (S) The public key for codes of the service provider equipment corresponding to desired service is delivered to client equipment at the time of service provision. The enciphered information which was received from client equipment is transmitted to service provider equipment. It has a means to transmit the enciphered information which was received from service provider equipment to client equipment. Client equipment (C) The data which become the session key for cryptocommunication between service provider equipment or the origin of this

session key are generated. It enciphers using the public key for codes which received a session key or data from authentication vicarious execution server equipment. After transmitting this enciphered information to authentication vicarious execution server equipment, the information which should be transmitted to service provider equipment is enciphered using a session key. It has a means to transmit this enciphered information to authentication vicarious execution server equipment. Service provider equipment (SP-A, SP-B) Decrypt the enciphered information which was received from authentication vicarious execution server equipment using the private key for codes, and acquire a session key, or data are acquired by the decryption using the private key for codes. After generating a session key from this data, the information which should be transmitted to client equipment is enciphered using a session key, and it has a means to transmit this enciphered information to authentication vicarious execution server equipment.

[0022] Moreover, authentication vicarious-execution server equipment has a means deliver the public key certificate for codes with the public key for codes in case the public key for codes is delivered to client equipment, as an example of 1 configuration of the authentication vicarious-execution service system of this invention, and client equipment has a means verify the public key for codes based on the public key certificate for codes received from authentication vicarious-execution server equipment, before performing encryption which used the public key for codes. As an example of 1 configuration of the authentication vicarious execution service system of this invention, moreover, client equipment In case it enciphers, the public key for codes is used, the authentication information on self-equipment is enciphered, and it has a means to transmit this enciphered information to authentication vicarious execution server equipment. Service provider equipment In case it decrypts, the enciphered information which was received from authentication vicarious execution server equipment is decrypted using the private key for codes, authentication information is acquired, and it has the means which attests client equipment based on this authentication information.

[0023] Moreover, at the time of service provision, the authentication vicarious execution server equipment (S) of this invention delivers the public key for codes of the service provider equipment corresponding to desired service to client equipment, and has a means to transmit the information enciphered in order to have made the decryption using the reception from client equipment, and the private key for codes of the information enciphered using this public key for codes perform to service provider equipment. Moreover, at the time of service provision, to the service provider equipment corresponding to desired service, the authentication vicarious execution server equipment (S) of this invention delivers the public key for codes of client equipment, and has a means transmit the information enciphered in order to have made the decryption using the reception from service provider equipment, and the private key for codes of the information enciphered using this public key for codes perform to client equipment.

[0024] Moreover, the authentication vicarious execution server equipment (S) of this invention The public key for codes of the service provider equipment corresponding to desired service is delivered to client equipment at the time of service provision. The data which become the session key for cryptocommunication enciphered using this public key for codes, or the origin of this session key From client equipment to reception After transmitting the session key or data enciphered in order to have made the decryption using the private key for codes perform to service provider equipment, While

transmitting the information from the client equipment enciphered using the session key to service provider equipment, it has a means to transmit the information from the service provider equipment enciphered using the session key to client equipment. Moreover, the example of 1 configuration of the authentication vicarious execution server equipment of this invention has a means to deliver the public key certificate for codes to client equipment with the public key for codes so that it may make the public key for codes verify to client equipment.

[0025] Moreover, while the client equipment (C) of this invention consists of an IC card equipped with a signature generation means to generate the signature for receiving client authentication from authentication vicarious execution server equipment An encryption means to encipher the information which should be transmitted to service provider equipment using the public key for codes, The signature generated with the IC card is transmitted to authentication vicarious execution server equipment. The public key for codes transmitted from authentication vicarious execution server equipment is received, and it outputs to an encryption means, and consists of a processor equipped with a transceiver means to transmit the information enciphered by the encryption means to authentication vicarious execution server equipment. Moreover, a signature generation means to generate a signature for the client equipment (C) of this invention to receive client authentication from authentication vicarious execution server equipment, While consisting of an IC card equipped with an encryption means to encipher the information which should be transmitted to service provider equipment using the public key for codes The signature generated with the IC card is transmitted to authentication vicarious execution server equipment. The public key for codes transmitted from authentication vicarious execution server equipment is received, and it outputs to an IC card, and consists of a processor equipped with a transceiver means to transmit the information enciphered with the IC card to authentication vicarious execution server equipment.

[0026]

[Embodiment of the Invention] [1 of the gestalt of operation], next the gestalt of operation of this invention are explained to a detail with reference to a drawing. Drawing 1 is the block diagram showing the configuration of the authentication vicarious execution service system used as the gestalt of operation of the 1st of this invention. The authentication vicarious execution service system of the gestalt of this operation In the above-mentioned conventional technique 2 or the above-mentioned conventional technique 3 Authentication vicarious execution server equipment S Two or more service provider equipments (It abbreviates to an authentication vicarious execution server hereafter) SP-A, public key PkSP-A of SP-B, and PkSP-B Client equipment (It abbreviates to a service provider hereafter) Deliver to C at the time of service provision, make the authentication vicarious execution server S encipher information to keep it secret by Client C side using this public key PkSP-A and PkSP-B, and it is made to return to the authentication vicarious execution server S. (It abbreviates to a client hereafter) Because the authentication vicarious execution server S transmits to service provider SP-A and SP-B and makes this information decrypt by private key SkSP-A and SkSP-B by service provider SP-A and SP-B Information transfer from Client C to service provider SP-A and SP-B is realized without revealing to the authentication vicarious execution server S.

[0027] Service provider SP-A, SP-B, and Client C are connected through a network, and

authentication vicarious execution server equipment S is formed in the middle of this network. drawing 1 -- setting -- PkSP-A and PkSP-B -- respectively -- service provider SP-A, the public key for codes of SP-B, SkSP-A, and SkSP-B -- they are service provider SP-A and the private key for codes of SP-B, respectively. Moreover, confidential information for SkU-A and SkU-B to receive service from service provider SP-A and SP-B, respectively and SkP are own confidential information of authentication vicarious execution server S. In the case of the method corresponding to the conventional technique 2 in the system of the gestalt of this operation, authentication of Client C is performed using confidential information SkU-A and SkU-B, and, in the case of the method corresponding to the conventional technique 3, authentication of Client C is performed using confidential information SkP.

[0028] Next, actuation of such an authentication vicarious execution service system is explained. While delivering public key PkSP-A for codes of suitable service provider SP-A to Client C according to the service whose client C requires the authentication vicarious execution server S at the time of service provision, a return demand of the information relevant to an encryption demand of the information using this public key PkSP-A and secrecy information which was signal-transduction-required and was enciphered in addition to this, and the changed information is given to Client C.

[0029] Here, in addition to this, a signal transduction demand is a demand of processing which changes secrecy information into the gestalt relevant to secrecy information which cannot be decrypted by service provider SP-A and SP-B, either, by service, only when required, it is advanced here, and it points out an one direction hash operation.

[0030] According to the demand of the authentication vicarious execution server S, Client C enciphers the information which should be transmitted to service provider SP-A using public key PkSP-A, and transmits the enciphered information to the authentication vicarious execution server S. Moreover, Client C transmits to the authentication vicarious execution server S with the information which enciphered the information which changed the hash operation etc., when [in relation to secrecy information] a signal transduction demand is made in addition to this.

[0031] The authentication vicarious execution server S performs a decryption demand to service provider SP-A while it transmits the information transmitted from Client C to reception and transmits this information to service provider SP-A. Service provider SP-A is decrypted using private key SkSP-A in which reception has the information transmitted from the authentication vicarious execution server S, and self has this information.

[0032] In this way, it can prevent that the information from Client C to service provider SP-A is revealed to the authentication vicarious execution server S, and partial solution of said trouble 1 is attained. In addition, although the above explanation of operation explains the case where service provision is performed by service provider SP-A, when service provision is performed by service provider SP-B, PkSP-B is used instead of public key PkSP-A, the information from Client C is transmitted to service provider SP-B, and service provider SP-B decrypts information using private key SkSP-B.

[0033] Moreover, it can omit because Client C performs autonomously a return demand of the information relevant to said encryption demand and secrecy information which was signal-transduction-required and was enciphered in addition to this, and the changed information, and similarly, it can omit because service provider SP-A and SP-B perform said decryption demand autonomously.

[0034] Moreover, in order to receive service provision from service provider SP-A and SP-B, the processings (generation of the signature by confidential information SkU-A, SkU-B, or SkP, service provider SP-A of this signature, transmission to SP-B, etc.) from which the authentication vicarious execution server S receives client authentication from service provider SP-A and SP-B instead of Client C as the above-mentioned conventional technique 2 or the above-mentioned conventional technique 3 explained are required. This processing may be performed to any at the time of delivering the information received from Client C to service provider SP-A and SP-B, or the time after said a series of sequences at the time before a series of sequences which result in a decryption of the information by service provider SP-A and SP-B from delivery of public key PkSP-A by the authentication vicarious execution server S, and PkSP-B.

[0035] [2 of gestalt of operation] drawing 2 is the block diagram showing the configuration of the authentication vicarious execution service system used as the gestalt of operation of the 2nd of this invention. The authentication vicarious execution service system of the gestalt of this operation It sets on the above-mentioned conventional technique 2 or the above-mentioned conventional technique 3, and the authentication vicarious execution server S is public key PkU' of Client C. - A and PkU'-B are delivered to service provider SP-A and SP-B. It is information to keep it secret from the authentication vicarious execution server S This public key PkU' - Make it encipher by the service provider SP-A and SP-B side using A and PkU'-B, and it is made to return to the authentication vicarious execution server S. The authentication vicarious execution server S transmits this information to Client C, and it is private key SkU' at Client C. - by making it decrypt by A and SkU'-B Information transfer to Client C is realized from service provider SP-A and SP-B, without revealing to the authentication vicarious execution server S.

[0036] drawing 2 -- setting -- CertU'-A, and the public key certificate for codes of the client [as opposed to service provider SP-A and SP-B in respectively -B] C and CertU'PkU'- A and PkU -- 'the public key for codes of the client [as opposed to service provider SP-A and SP-B in respectively -B] C, and SkU' -A and SkU' -B is the private key for codes of the client C to service provider SP-A and SP-B, respectively. In the case of the method corresponding to the conventional technique 2 in the system of the gestalt of this operation, authentication of Client C is performed using confidential information SkU-A and SkU-B, and, in the case of the method corresponding to the conventional technique 3, authentication of Client C is performed using confidential information SkP.

[0037] Next, actuation of such an authentication vicarious execution service system is explained. suitable service provider SP-A according to the service whose client C requires the authentication vicarious execution server S at the time of service provision -- receiving -- public key PkU'-A for codes of Client C -- public key certificate CertUfor codes' -- while delivering in the form added to -A -- this public key PkU' -- an encryption demand of the information using -A is performed.

[0038] By the demand of this authentication vicarious execution server S, service provider SP-A enciphers the information which should be transmitted to Client C using public key certificate CertU 'public key PkU contained in -A' for codes-A, and transmits the enciphered information to the authentication vicarious execution server S. The authentication vicarious execution server S performs a decryption demand to Client C while it transmits the information transmitted from service provider SP-A to reception

and transmits this information to Client C.
[0039] Client C is decrypted using private key SkU'-A in which reception has the information transmitted from the authentication vicarious execution server S, and self has this information. In this way, it can prevent that the information on Client C is revealed to the authentication vicarious execution server S from service provider SP-A, and partial solution of said trouble 1 is attained. In addition, although the above explanation of operation explains the case where service provision is performed by service provider SP-A, when service provision is performed by service provider SP-B, it is CertU', respectively instead of certificate CertU'-A and public key PkU'-A. - B and PkU'-B are used, the information from service provider SP-B is transmitted to Client C, and Client C decrypts information using private key SkU'-B.
[0040] Moreover, it can omit because service provider SP-A and SP-B perform said encryption demand autonomously, and similarly, it can omit because Client C performs said decryption demand autonomously. With the gestalt of this operation, must manage private key SkU'-A and SkU'-B by Client C, and a private key is needed for every service, however it is private key SkU'. - Management of public key certificate CertU'-A, CertU'-B corresponding to A and SkU'-B can entrust the authentication vicarious execution server S. therefore, the authentication vicarious execution server S -- it is -- /-- it is not concerned nothing but the application to the service which needs the private key for codes primarily is effective.
[0041] moreover The processings (generation of the signature by confidential information SkU-A, SkU-B, or SkP, service provider SP-A of this signature, transmission to SP-B, etc.) from which the authentication vicarious execution server S receives client authentication from service provider SP-A and SP-B instead of Client C Public key PkU' by the authentication vicarious execution server S - You may carry out to any at the time before a series of sequences from delivery of A and PkU'-B to a decryption of the information by Client C, and after said a series of sequences.
[0042] [3 of gestalt of operation] drawing 3 is the block diagram showing the configuration of the authentication vicarious execution service system used as the gestalt of operation of the 3rd of this invention. The authentication vicarious execution service system of the gestalt of this operation In 1 of the gestalt of operation at the time of the delivery to the client C of public key PkSP-A for codes, and PkSP-B Generation of the data which become the origin of generation of a session key or a session key is required from Client C. The information which was made to return after making these encipher using public key PkSP-A for codes, and PkSP-B furthermore, and was enciphered by transmitting to service provider SP-A and SP-B Bidirectional information transfer between Client C, service provider SP-A, and SP-B is realized without revealing to the authentication vicarious execution server S.
[0043] In drawing 3 , SSkA and SSkB(s) are data, such as a random number with which the session key for cryptocommunication between Client C and service provider SP-B, SdSSKA, and SdSSkB become the origin of generation of the session keys SSkA and SSkB for cryptocommunication between Client C and service provider SP-A, respectively. In the case of the method corresponding to the conventional technique 2 in the system of the gestalt of this operation, authentication of Client C is performed using confidential information SkU-A and SkU-B, and, in the case of the method corresponding to the conventional technique 3, authentication of Client C is performed using

confidential information SkP.
[0044] Next, actuation of such an authentication vicarious execution service system is explained. While delivering public key PkSP-A for codes of suitable service provider SP-A to Client C according to the service whose client C requires the authentication vicarious execution server S at the time of service provision, a return demand of the information which the session key SSkA or Data SdSSKA using the generation demand of the data SdSSKA which become the origin of the generation demand of the session key SSkA for cryptocommunication or the session key SSkA, and public key PkSP-A was encryption-required, and was enciphered is given to Client C.
[0045] By the demand of this authentication vicarious execution server S, Client C generates the session key SSkA for cryptocommunication. Moreover, Client C generates the data SdSSKA which become the origin of the session key SSkA depending on the case. And Client C enciphers the session key SSkA or Data SdSSKA using public key PkSP-A, and transmits the enciphered information to the authentication vicarious execution server S.
[0046] If it is required, the authentication vicarious execution server S will require generation of the session key SSkA for cryptocommunication from service provider SP-A from Data SdSSKA, while it transmits the information transmitted from Client C to reception and transmits this information to service provider SP-A.
[0047] Service provider SP-A is decrypted using private key SkSP-A in which reception has the information transmitted from the authentication vicarious execution server S, and self has this information, and acquires the session key SSkA. Moreover, when generation of the session key SSkA is required from the authentication vicarious execution server S, service provider SP-A decrypts the information transmitted from the authentication vicarious execution server S using private key SkSP-A, acquires Data SdSSKA, and generates the session key SSkA from this data SdSSKA.
[0048] Henceforth, the exchange of information safe about the bidirectional communication link between Client C and service provider SP-A is attained. That is, when transmitting information to service provider SP-A from Client C, service provider SP-A which Client C transmitted the information which should be transmitted after enciphering using the session key SSkA, and received the enciphered information through the authentication vicarious execution server S decrypts information using the session key SSkA which self has.
[0049] On the other hand, when transmitting information to Client C from service provider SP-A, service provider SP-A transmits the information which should be transmitted, after enciphering using the session key SSkA, and the client C which received the enciphered information through the authentication vicarious execution server S decrypts information using the session key SSkA which self has.
[0050] In this way, it becomes possible to prevent not only the information from Client C to service provider SP-A but that information is revealed to the authentication vicarious execution server S in the information delivery to Client C from service provider SP-A. In addition, although the above explanation of operation explains the case where service provision is performed by service provider SP-A, when service provision is performed by service provider SP-B, PkSP-B, the session key SSkB, and Information SdSSKB are used instead of public key PkSP-A, the session key SSkA, and Data SdSSKA, respectively, the information from Client C is transmitted to service provider SP-B, and service provider

SP-B generates the session key SSkB from Data SdSSKB.
[0051] Moreover, it can omit because Client C performs autonomously a return demand of said information which was generation-required, was encryption-required and was enciphered, and similarly, it can omit because service provider SP-A and SP-B perform said generation demand autonomously.
[0052] moreover The processings (generation of the signature by confidential information SkU-A, SkU-B, or SkP, service provider SP-A of this signature, transmission to SP-B, etc.) from which the authentication vicarious execution server S receives client authentication from service provider SP-A and SP-B instead of Client C The time before a series of sequences from delivery of public key PkSP-A by the authentication vicarious execution server S, and PkSP-B to generation of the session key SSkA by service provider SP-A and SP-B, The enciphered session keys SSkA and SSkB or Data SdSSKA and SdSSkB may be performed to any at the time of delivering to service provider SP-A and SP-B, or the time after said a series of sequences.
[0053] [4 of gestalt of operation] drawing 4 is the block diagram showing the configuration of the authentication vicarious execution service system used as the gestalt of operation of the 4th of this invention. In 3 of the gestalt of 1 or operation of the gestalt of operation, the problem who verifies service provider SP-A, public key PkSP-A for codes of SP-B, and PkSP-B how exists. For example, when verification (for example, verification of a certificate authority signature of a public key certificate, the check of CRL, etc.) of public key PkSP-A and PkSP-B is entrusted to the authentication vicarious execution server S, the following problems arise.
[0054] Namely, a fake public key is delivered from the authentication vicarious execution server S to Client C. After decrypting the information from Client C to service provider SP-A and SP-B using the private key corresponding to a fake public key which the authentication vicarious execution server S recognizes If actuation of enciphering this decrypted information using right public key PkSP-A and PkSP-B anew, and transmitting to service provider SP-A and SP-B is performed, it will become possible to acquire information unjustly in the authentication vicarious execution server S.
[0055] Then, the authentication vicarious execution service system of the gestalt of this operation requires verification of service provider SP-A, public key PkSP-A for codes of SP-B, and PkSP-B from Client C from the authentication vicarious execution server S. That is, the authentication vicarious execution server S delivers public key certificate CertSP-A for codes, and CertSP-B to Client C with public key PkSP-A for codes, and PkSP-B.
[0056] Client C holds the certificate of for example, a high order certificate authority to every service provider SP-A and SP-B, and verifies public key certificate CertSP-A and CertSP-B which have been delivered from the authentication vicarious execution server S using the certificate of a high order certificate authority. Moreover, Client C performs the check of whether public key certificate CertSP-A and CertSP-B are invalidated based on a certificate cancellation list (it abbreviates to CRL Certificate Revocation List and the following).
[0057] In this way, verification of public key PkSP-A for codes and PkSP-B can be performed. In addition, the authentication vicarious execution server S can fully be trusted for Client C, and it is not necessary to take into consideration delivering a fake public key to Client C in many cases. That is, although it generally cannot be trusted

about the information leak concerning the bidirectional communication link between Client C, service provider SP-A, and SP-B, it says in many cases that it is not necessary to take into consideration about fake public key delivery, and 1 of the gestalt of operation or 3 is enough.

[0058] The reason is easy [activation] rather than the direction robbed of the information which becomes a plaintext within Server S performs a series of malfeasances by fake public key delivery for the external invader who accesses unjustly the employment operator of the authentication vicarious execution server S, and the authentication vicarious execution server S. Moreover, said verification demand is omissible because Client C verifies a public key autonomously.

[0059] [5 of gestalt of operation] drawing 5 is the block diagram showing the configuration of the authentication vicarious execution service system used as the gestalt of operation of the 5th of this invention. The authentication vicarious execution service system of the gestalt of this operation In 1 of the gestalt of operation, or the system of 3, delivery of the information on service provider SP-A from Client C enciphered using public key PkSP-A and PkSP-B and SP-B is used. The authentication information on a form whose decryption is impossible for Client C in the authentication vicarious execution server S is required, this authentication information is transmitted to service provider SP-A and SP-B from the authentication vicarious execution server S, and client authentication is performed by service provider SP-A and SP-B.

[0060] In drawing 5 , A and B are the authentication information on the client C corresponding to service provider SP-A and SP-B, respectively. In case the authentication vicarious execution server S delivers public key PkSP-A for codes, and PkSP-B to Client C, it gives an encryption demand of the authentication information A and B using this public key PkSP-A and PkSP-B to Client C.

[0061] In case Client C enciphers the information which should be transmitted to service provider SP-A using public key PkSP-A, it uses public key PkSP-A, enciphers the authentication information (password) A, and transmits to the authentication vicarious execution server S with other information that it explained by 1 of the gestalt of operation of this enciphered authentication information A, or 3. Similarly, in case Client C enciphers the information which should be transmitted to service provider SP-B using public key PkSP-B, it uses public key PkSP-B, enciphers the authentication information (password) B, and transmits to the authentication vicarious execution server S with other information that it explained by 1 of the gestalt of operation of this enciphered authentication information B, or 3.

[0062] Reception is used for service provider SP-A and SP-B for the information which was transmitted from Client C and transmitted by the authentication vicarious execution server S, and private key SkSP-A for codes and SkSP-B are used for them for this information, they decrypt, and acquire the authentication information A and B. And service provider SP-A and SP-B attest Client C based on the authentication information A and B.

[0063] In this way, the authentication vicarious execution server S can prevent becoming Client C and clearing up, and can solve said trouble 2. Moreover, even if the authentication vicarious execution server S receives client authentication by the own confidential information SkP, it becomes direct authentication of Client C is possible, and possible to have the means which prevents the authentication vicarious execution server's

S becoming Client C, and clearing up, and to make the responsibility for the authentication vicarious execution server S mitigate of service provider SP-A and SP-B (solution of said trouble 3).

[0064] Since one of the advantages using the authentication vicarious execution server S is decreasing the number of the confidential information managed by Client C, the authentication information A and B on the gestalt of this operation becomes common [considering as a simple thing compared with what is managed by the authentication vicarious execution server S]. For example, the authentication vicarious execution server S performs client authentication processing in which confidential information SkU-A, SkU-B, or SkP was used, and client authentication is received by sending Client C to service provider SP-A and SP-B in the form kept secret from the authentication vicarious execution server S by making a password simpler than said confidential information into authentication information.

[0065] In addition, since the Replay attack by the authentication vicarious execution server S is attained when transmitting the same password each time, it is also effective to transmit combining a serial value, time information, or the session key explained by 3 of the gestalt of operation and authentication information.

[0066] [6 of gestalt of operation] drawing 6 is the block diagram showing the configuration of the authentication vicarious execution server S used as the gestalt of operation of the 6th of this invention. The authentication vicarious execution server S shown in drawing 6 realizes the authentication vicarious execution service system of 1-5 of the gestalt of operation. The authentication vicarious execution server S has the authentication function of Client C, and a public key delivery function for codes at least, and, in other than three of the gestalt of operation, has a public key certificate verification function for codes.

[0067] In addition, when the method of the conventional technique 2 performs processing from which the authentication vicarious execution server S receives client authentication from service provider SP-A and SP-B instead of Client C, the SkP storage machine 10 and the CertP storage machine 11 are unnecessary, and when the method of the conventional technique 3 performs, the SkU-A storage machine 8 and the CertU-A storage machine 9 are unnecessary.

[0068] Memorizing confidential information SkU-P for using the SkU-P storage machine 1 for authentication between the authentication vicarious execution server S and Client C, the CertU-P storage machine 2 has memorized certificate CertU-P corresponding to confidential information SkU-P. Confidential information SkU-P and certificate CertU-P are memorized for every client C.

[0069] The SkU-P verification machine 3 attests Client C with reference to the SkU-P storage machine 1 and the CertU-P storage machine 2 based on confidential information SkU-P which was transmitted from Client C and received by the transmitter-receiver 14, certificate CertU-P, or confidential information SkU-P and certificate CertU-P. Generally, the SkU-P verification machine 3 is referring to the identification number of each client C, and the conversion table of each confidential information SkU-P, and attests Client C.

[0070] The SP-A public key storage machine 4 memorized public key PkSP-A for codes, and PkSP-B (PkU' - A, PkU' - B), the SP-A public key certificate CRL storage machine 5 memorized public key certificate CertSP-A corresponding to this public key for codes,

and CRL of CertSP-B (CertU' - A, CertU' - B), and the SP-A high order certificate authority public key certificate storage machine 6 has memorized the public key certificate of a high order certificate authority. The public key for codes, CRL, and the public key certificate of a high order certificate authority are memorized by each service provider SP-A and every SP-B.
[0071] SP public key certificate verification machine 7 verifies the public key for codes with reference to the SP-A public key storage machine 4, the SP-A public key certificate CRL storage machine 5, and the SP-A high order certificate authority public key certificate storage machine 6. In addition, although not illustrated in drawing 6 , a means to acquire CRL, and a means to acquire a high order certificate authority public key certificate are needed separately in fact.
[0072] The SkU-A storage machine 8 memorized confidential information SkU-A and SkU-B, and the CertU-A storage machine 9 has memorized confidential information SkU-A, certificate CertU-A corresponding to SkU-B, and CertU-B. Confidential information SkU-A, SkU-B, and certificate CertU-A and CertU-B are memorized for every service provider SP-A, SP-B, and every client C.
[0073] The SkP storage machine 10 memorized the own confidential information SkP of server S, and the CertP storage machine 11 has memorized the certificate CertP corresponding to confidential information SkP. The signature generation machine 12 generates the signature which enciphered predetermined correspondence using confidential information SkU-A, SkU-B, or SkP, and transmits this signature to service provider SP-A and SP-B through a transmitter-receiver 14. Depending on the case, the signature generation machine 12 transmits certificate CertU-A, CertU-B, or CertP to service provider SP-A and SP-B with said signature.
[0074] The vicarious execution processing section 13 performs vicarious execution processings other than the processing explained by 1-5 of the gestalt of operation if needed. It connects with Client C and service provider SP-A, and SP-B through a network, and a transmitter-receiver 14 transmits and receives information between Client C and service provider SP-A, and SP-B.
[0075] In addition, although what is depended on the authentication method which used public key encryption as client authentication is assumed with the gestalt of this operation, depending on an authentication method, the signature generation machine 12, the SkU-P verification machine 3, and the storage machines 5, 6, 9, and 11 of certificate Cert(s) become unnecessary. For example, in password authentication, a certificate does not have the need and its signature generation machine 12 is also unnecessary.
[0076] The above authentication vicarious execution servers S can be installed as the gateway of broader-based network WAKUHE, such as the Internet, from the inside LAN of the server on [, such as the Internet top,] a network, and a company, and domestic [LAN], for example, are realized as the software, the hardware, and the peripheral device on a workstation, a personal computer, a router, a terminal adopter, etc.
[0077] [7 of gestalt of operation] drawing 7 is the block diagram showing the configuration of Client C used as the gestalt of operation of the 7th of this invention. The client C shown in drawing 7 realizes the authentication vicarious execution service system of 1-5 of the gestalt of operation. Client C has a public key reception function for codes, and an encryption function by the public key for codes at least, and, in the case of 2 of the gestalt of operation, in the case of 3 of the gestalt of the decryption function by

the private key for client codes, and implementation, has a public key certificate verification function for codes in the case of 4 of the gestalt of session key generation / transmitting function and encryption/decryption function by the session key, and implementation.

[0078] That is, in other than two of the gestalt of operation, the SkU'-A storage machine 26 and the decoder 27 are unnecessary, in other than three of the gestalt of operation, they are unnecessary, and, in other than four of the gestalt of operation, the SP public key certificate CRL storage machine 32, SP high order certificate authority public key certificate storage machine 33, and SP public key certificate verification machine 34 are unnecessary [the decoder] to them. [of the SSk generation machine 28, the SSk temporary storage machine 29, the SdSSK generation machine 30, and encryption/decryption machine 31]

[0079] Memorizing confidential information SkU-P for using the SkU-P storage machine 21 for authentication between the authentication vicarious execution server S and the self-client C, the CertU-P storage machine 22 has memorized certificate CertU-P corresponding to confidential information SkU-P. The signature generation machine 23 generates the signature which enciphered predetermined correspondence using confidential information SkU-P, and transmits this signature to the authentication vicarious execution server S through a transmitter-receiver 36. Depending on the case, the signature generation machine 23 transmits certificate CertU-P to the authentication vicarious execution server S with said signature.

[0080] SP public key temporary storage machine 24 has memorized public key PkSP-A for codes and PkSP-B which were transmitted from the authentication vicarious execution server S, and were received by the transmitter-receiver 36. The encryption machine 25 enciphers information using this public key PkSP-A for codes, and PkSP-B, and transmits the enciphered information to the authentication vicarious execution server S through a transmitter-receiver 36.

[0081] The SkU'-A storage machine 26 is private key SkUfor codes'. - A and SkU'-B are memorized. This private key for codes is memorized for every service provider SP-A and SP-B. A decoder 27 is the information which was transmitted from the authentication vicarious execution server S, and was received by the transmitter-receiver 36 Private key SkUfor codes' - It decrypts using A and SkU'-B.

[0082] The SSk generation machine 28 generates the session keys SSkA and SSkB for cryptocommunication, and the SSk temporary storage machine 29 memorizes these session keys SSkA and SSkB for cryptocommunication. The SdSSK generation machine 30 generates the data SdSSKA and SdSSkB which become the origin of the session keys SSkA and SSkB.

[0083] Encryption/decryption machine 31 enciphers the information which should be transmitted using the session keys SSkA and SSkB, and transmits the enciphered information to the authentication vicarious execution server S through a transmitter-receiver 36. Moreover, encryption/decryption machine 31 decrypts the enciphered information which was transmitted from the authentication vicarious execution server S, and was received by the transmitter-receiver 36 using the session keys SSkA and SSkB.

[0084] The SP public key certificate CRL storage machine 32 memorized public key PkSP-A for codes, public key certificate CertSP-A corresponding to PkSP-B, and CRL of CertSP-B, and SP high order certificate authority public key certificate storage machine

33 has memorized the public key certificate of a high order certificate authority. CRL and the public key certificate of a high order certificate authority are memorized for every service provider SP-A and SP-B.
[0085] SP public key certificate verification machine 34 performs verification of public key PkSP-A for codes and PkSP-B which were transmitted from the authentication vicarious execution server S, and were received by the transmitter-receiver 36 with reference to the SP public key certificate CRL storage machine 32 and SP high order certificate authority public key certificate storage machine 33. In addition, although not illustrated in drawing 7 , a means to acquire CRL, and a means to acquire a high order certificate authority public key certificate are needed separately in fact.
[0086] I/O device 35 outputs information to a user while outputting these directions to each configuration in Client C, if the directions from the user of Client C are inputted. It connects with the authentication vicarious execution server S through a network, and a transmitter-receiver 36 transmits and receives information between the authentication vicarious execution servers S.
[0087] In addition, also in the gestalt of this operation, although the client authentication function to the authentication vicarious execution server S assumes the public key cryptosystem, the circuit which becomes unnecessary depending on an authentication method exists. The above client equipments C are realized as software on a personal computer. Moreover, it is also possible to realize a part or all functions on safe devices, such as a smart card (IC card).
[0088] For example, the function of the SkU-P storage machine 21, the CertU-P storage machine 22, and the signature generation machine 23 is given to a smart card. The computer equipped with the reader/writer function of a smart card for the remaining function, It is possible to give processors, such as telephone or a set top box. It is also possible to give the function of SP public key temporary storage machine 24 and the encryption machine 25 to a smart card with the function of the SkU-P storage machine 21, the CertU-P storage machine 22, and the signature generation machine 23, and to give the remaining function to a processor.
[0089] [8 of gestalt of operation] drawing 8 and drawing 9 are the sequence diagrams showing actuation of the authentication vicarious execution service system used as the gestalt of operation of the 8th of this invention. The authentication vicarious execution service system of the gestalt of this operation applies the system explained by 5 of the gestalt of operation to server management mold Wallet for network DEBITTO settlement of accounts.
[0090] Here, as a method of network DEBITTO settlement of accounts, SET (Online PIN Extension is included) or SECE is assumed. Although it becomes dealings between 3 persons of a user, a member's store, and the financial institution gateway in network DEBITTO settlement of accounts, server management mold Wallet is software which operates on the server generally installed on the network, in order to mitigate the processing burden of a user's client SOFUTOHE. Now, server management mold Wallet announced will be equivalent to the conventional technique 2, and will be able to see the personal identification number (PIN) of the bank account which the user inputted by the server to which Sir BAWO let operates. Even if it enciphers between a user and server management mold Wallet, in order to create the wording of a telegram which transmits to a member's store, it will decrypt once.

[0091] Then, the system explained by 5 of the gestalt of operation is applied to server management mold Wallet for network DEBITTO settlement of accounts. Hereafter, actuation of the system of the gestalt of this operation is explained using drawing 8 and drawing 9 . For PGW, in drawing 8 and drawing 9 , a bank server (service provider) and M are [Sir BAWO let (authentication vicarious execution server equipment) and AS of a member's store and SW] authentication servers (for authentication between Client C and an authentication vicarious execution server).
[0092] First, if an IC card is inserted in Client C, Client C pays and a user pushes a carbon button as shown in drawing 8 , the initiation which shows dealings initiation from a member's store M will be sent to Client C. Then, a user's input of a card password performs authentication of an IC card by authentication server AS. Client C requires a service log in from authentication server AS after authentication. Thereby, service starts.
[0093] The menu which asks a user's account from the Sir BAWO let SW is sent after service starting. A user operates Client C and specifies a desired account. If the information which specifies a user's account is sent to the Sir BAWO let SW, the Sir BAWO let SW will perform initialization processing of predetermined between the bank servers PGW.
[0094] Next, as shown in drawing 9 , the Sir BAWO let SW transmits account information, a PGW public key (equivalent to public key PkSP-A for codes, and PkSP-B), and the information on other (SET/SECE PIHead) to Client C. A user inputs PIN (equivalent to a personal identification number A and B, i.e., the authentication information of 5 on the gestalt of operation) into Client C. Here, in SET/SECE, since what changed the data format of PIN or PIN into the field called PANData is contained, this is assembled in Client C.
[0095] And PIN information calculates the PIN related code data H (PIHead+PANData), H (PANData), and E (PkPGW, PANData+K) in Client C, in order to notify only to the bank server PGW which is a service provider and to keep it secret to the Sir BAWO let SW. H() here shows a hash operation and E() shows a RSA operation. In this way, the PIN information enciphered with the PGW public key is sent to the bank server PGW.
[0096] A member's store M and the bank server SW are good with a function as usual by doubling with the wording-of-a-telegram format from the wording of a telegram from the usual client C, or conventional server management mold Wallet about the wording of a telegram to a member's store M from the Sir BAWO let SW.
[0097] Thereby, in a Sir BAWO let entrepreneur, it can become difficult to decode a bank account PIN and it can decrease the risk which a bank account PIN reveals. Moreover, when a financial institution has a means to attest a user directly by PIN, clarification of the responsibility whereabouts between a financial institution when injustice etc. occurs, a Sir BAWO let entrepreneur, and a user becomes easy. In addition, with the gestalt of this operation, it is possible not to add modification to the wording of a telegram between the client when not using an authentication vicarious execution server, a member's store and a member's store, and a bank server.
[0098] Moreover, with the gestalt of this operation, a smart card is distributed to a user and it assumes using for the mutual recognition between a client and a Sir BAWO let entrepreneur server. SSL (Secure Sockets Layer) server authentication or the SSL mutual recognition in the gestalt which stored the client certificate of attestation on the hard disk may be used. Also when forgery generally uses a difficult smart card and a bank account

PIN is temporarily revealed to others in a user's management mistake, the risk by which accounts will be settled by becoming a limitation without the copy and theft of a smart card, and clearing up becomes however, there are less, [few] Moreover, when most PIN-related processings will be performed within a smart card when the above-mentioned smart card is used as a thing equivalent to the client C of this invention, and cooperative use of a terminal etc. is considered, it is possible to raise safety more.

[0099] [9 of gestalt of operation] drawing 10 is the sequence diagram showing actuation of the authentication vicarious execution service system used as the gestalt of operation of the 9th of this invention. The authentication vicarious execution service system of the gestalt of this operation applies the system explained by 5 of the gestalt of operation to server management mold Wallet's customer certification dictation profit in network DEBITTO settlement of accounts.

[0100] In addition, in drawing 10 , about a part for the sequence first portions, such as authentication between Client C and the Sir BAWO let SW, since it is fundamentally the same as that of 8 of the gestalt of operation, it omits. In SECE etc., before applying for a customer certificate to a customer certificate authority, the customer specification personal identification number comes to hand by mail etc. from the financial institution etc. This is described in an application at the time of the application to a customer certificate authority, and a customer certificate authority sets this justification to one of the examination items. That is, the customer certificate authority will attest the customer by this customer specification personal identification number (it has not necessarily attested only by this number and carries out by, of course combining the check of the contents of description of an application etc.).

[0101] In conventional server management mold Wallet, there is a problem of the leakage to the Sir BAWO let entrepreneur of a customer specification personal identification number like 8 of the gestalt of operation. For example, a Sir BAWO let entrepreneur's employment person does the theft of this, when it becomes a customer and clears up, it comes to make renewal of a customer private key and a corresponding certificate, and there is a possibility that it may clear up and DEBITTO settlement of accounts may be performed.

[0102] Then, the system explained by 5 of the gestalt of operation is applied to server management mold Wallet for network DEBITTO settlement of accounts. Hereafter, actuation of the system of the gestalt of this operation is explained using drawing 10 . In drawing 10 , CCA is a customer certificate authority. First, the Sir BAWO let SW requires and acquires an application to the customer certificate authority CCA. And the Sir BAWO let SW transmits a CCA public key (equivalent to public key PkSP-A for codes, and PkSP-B) to Client C with this application.

[0103] A user inputs a customer specification personal identification number into Client C. Client C enciphers this customer specification personal identification number using a CCA public key, and transmits the enciphered information to the Sir BAWO let SW. The Sir BAWO let SW is transmitted to the customer certificate authority CCA, after giving a customer signature to information from Client C.

[0104] The customer certificate authority CCA decrypts the enciphered information which was received from the Sir BAWO let SW with a CCA private key, acquires a customer specification personal identification number, and attests a user based on this customer specification personal identification number. The customer certificate authority

CCA transmits a certificate to the Sir BAWO let SW after authentication.
[0105] As mentioned above, in order to encipher a customer specification personal identification number and to transmit, the decode by the Sir BAWO let entrepreneur becomes difficult. In order to prevent the Replay attack by the Sir BAWO let entrepreneur, it is desirable to include a value which is different at [, such as a serial number,] every application in addition to a customer specification personal identification number in the candidate for encryption. In addition, in the case of the gestalt of this operation, in addition to the function of the customer certificate authority CCA in the SECE specification by which September, Heisei 11 current public presentation is carried out, it is newly [the decryption function of the customer specification personal identification number by the private key for customer certificate authority encryption] needed in the customer certificate authority CCA.
[0106] [10 of gestalt of operation] drawing 11 and drawing 12 are the sequence diagrams showing actuation of the authentication vicarious execution service system used as the gestalt of operation of the 10th of this invention. The authentication vicarious execution service system of the gestalt of this operation is applied as an authentication vicarious execution server of SSL authentication of the system explained by 3 of the gestalt of operation. The gestalt of this operation performs SSL mutual recognition, and encryption algorithm assumes RSA.
[0107] Between a client and a SSL server, when performing the conventional SSL authentication, confidential information, such as a user's certificate, a private key, etc., is needed for a client. Since a cost risk etc. follows on confidential information management of a user in many cases as above-mentioned, in order to lessen a user's confidential information as much as possible, suppose that an authentication vicarious execution server is used. However, since all the encryption information on SSL will be created with an authentication vicarious execution server instead of a client when making all SSL authentications perform by the authentication vicarious execution server, it becomes possible to create the common key between a SSL server and a client by the authentication vicarious execution server. Now, all confidential information will leak to an authentication vicarious execution server.
[0108] Then, if 3 of the gestalt of operation is applied, at the time of a communication link, it will encipher with the public key of a SSL server, and will transmit to an authentication vicarious execution server so that it may be made to carry out by the client about generation of the Prima star secret which becomes a SSL server and the origin of the confidential information which it has between clients, and a master secret and cannot see by the authentication vicarious execution server about the Prima star secret. Moreover, about the signature of the client demanded from a SSL server, the digest is created by the client, it transmits to an authentication vicarious execution server, and an authentication vicarious execution server signs with a user's private key. SSL authentication is attained without a user's confidential information leaking to an authentication vicarious execution server by carrying out like this.
[0109] Hereafter, actuation of the system of the gestalt of this operation is explained using drawing 11 and drawing 12 . First, if a user inserts an IC card in Client C and enters a card password as shown in drawing 11 , authentication of an IC card will be performed by the authentication vicarious execution server S. Client C requires a service log in from the authentication vicarious execution server S after authentication. Thereby, service

starts.
[0110] The authentication vicarious execution server S performs initialization processing of predetermined between SSL servers, after service starting. Next, as shown in drawing 12 , the authentication vicarious execution server S transmits a server public key (equivalent to public key PkSP-A for codes, and PkSP-B) to Client C while requiring a client key (Client Key) from Client C.
[0111] Client C generates the Prima star secret (equivalent to Data SdSSKA and SdSSkB), enciphers this Prima star secret using a server public key, and transmits the enciphered information to the authentication vicarious execution server S. In this way, the Prima star secret enciphered with the server public key is sent to a SSL server. Furthermore, Client C transmits the information which generated the master secret based on the Prima star secret, performed the hash operation to this master secret, and performed this hash operation to the authentication vicarious execution server S.
[0112] As mentioned above, although almost all the parts in SSL authentication can be performed by the authentication vicarious execution server S, about the part which generates the Prima star secret which is the part which a user wants to make secret to the authentication vicarious execution server S, and a master secret, it is generable by Client C by giving required information from the authentication vicarious execution server S.
[0113] About the other part, the authentication vicarious execution server S takes over all communication links with a SSL server. By sending the part of "Finished" shown in drawing 12 to Client C, the encryption communication link (equivalent to the encryption communication link using the session key explained by 3 of the gestalt of operation) in both directions can be started. In the communication link, it can communicate between a SSL server and Client C, without revealing the contents of a communication link, since the authentication vicarious execution server S does not know the common key which it has by the SSL server and Client C.
[0114]
[Effect of the Invention] According to this invention, authentication vicarious execution server equipment delivers the public key for codes of the service provider equipment corresponding to desired service to client equipment. The enciphered information which was received from client equipment is transmitted to service provider equipment. Client equipment enciphers the information which should be transmitted to service provider equipment using the public key for codes. When this enciphered information is transmitted to authentication vicarious execution server equipment and service provider equipment decrypts the enciphered information which was received from authentication vicarious execution server equipment using the private key for codes Information transfer from client equipment to service provider equipment can be performed without revealing to authentication vicarious execution server equipment.
[0115] Moreover, authentication vicarious execution server equipment receives the service provider equipment corresponding to desired service. Deliver the public key for codes of client equipment, and the enciphered information which was received from service provider equipment is transmitted to client equipment. Service provider equipment enciphers the information which should be transmitted to client equipment using the public key for codes. When this enciphered information is transmitted to authentication vicarious execution server equipment and client equipment decrypts the enciphered information which was received from authentication vicarious execution

server equipment using the private key for codes Information transfer from service provider equipment to client equipment can be performed without revealing to authentication vicarious execution server equipment.
[0116] Moreover, authentication vicarious execution server equipment delivers the public key for codes of the service provider equipment corresponding to desired service to client equipment. The enciphered information which was received from client equipment is transmitted to service provider equipment. The enciphered information which was received from service provider equipment is transmitted to client equipment. The data with which client equipment becomes the session key for cryptocommunication between service provider equipment or the origin of this session key are generated. After enciphering a session key or data using the public key for codes and transmitting this enciphered information to authentication vicarious execution server equipment, The information which should be transmitted to service provider equipment is enciphered using a session key. This enciphered information is transmitted to authentication vicarious execution server equipment. Service provider equipment Decrypt the enciphered information which was received from authentication vicarious execution server equipment using the private key for codes, and acquire a session key, or data are acquired by the decryption using the private key for codes. By enciphering the information which should be transmitted to client equipment using a session key, and transmitting this enciphered information to authentication vicarious execution server equipment, after generating a session key from this data Bidirectional information transfer between client equipment and service provider equipment can be performed without revealing to authentication vicarious execution server equipment.
[0117] Moreover, since the public key for codes is verified based on the public key certificate for codes received from authentication vicarious execution server equipment before delivering the public key certificate for codes with the public key for codes and performing encryption using the public key for codes of client equipment, in case authentication vicarious execution server equipment delivers the public key for codes to client equipment, the public key for codes delivered from authentication vicarious execution server equipment is verifiable.
[0118] Moreover, in case client equipment enciphers, use the public key for codes and the authentication information on self-equipment is enciphered. This enciphered information is transmitted to authentication vicarious execution server equipment. Service provider equipment Since the enciphered information which was received from authentication vicarious execution server equipment is decrypted using the private key for codes, authentication information is acquired and client equipment is attested based on this authentication information in case it decrypts Authentication vicarious execution server equipment can prevent becoming client equipment and clearing up, and it becomes possible to make the responsibility for authentication vicarious execution server equipment mitigate further of it.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－134534
（P2001－134534A）
(43)公開日　平成13年５月18日(2001.5.18)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｅ	５Ｂ０８５
13/00	３５１	13/00	３５１Ｚ	５Ｂ０８９

審査請求　未請求　請求項の数16　ＯＬ　（全 27 頁）

(21)出願番号　特願平11－317468

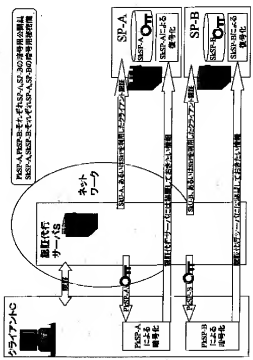
(22)出願日　平成11年11月８日(1999.11.8)

(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町－丁目１番６号
(72)発明者　疋田　智治
東京都千代田区内幸町－丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(74)代理人　100064621
弁理士　山川　政樹

最終頁に続く

(54)【発明の名称】　認証代行方法、認証代行サービスシステム、認証代行サーバ装置及びクライアント装置

(57)【要約】
【課題】　クライアント認証を代行する認証代行サーバに情報が漏洩することを防止する。
【解決手段】　認証代行サーバＳは、サービス提供時、所望のサービスに対応したサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂの暗号用公開鍵をクライアントＣへ配送し、クライアントＣから受け取った暗号化された情報をプロバイダＳＰ－Ａ，ＳＰ－Ｂへ転送する。クライアントＣは、プロバイダＳＰ－Ａ，ＳＰ－Ｂへ送信すべき情報を認証代行サーバＳから受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバＳへ送信する。プロバイダＳＰ－Ａ，ＳＰ－Ｂは、認証代行サーバＳから受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する。



【特許請求の範囲】

【請求項1】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられた認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行方法において、

サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置の暗号用公開鍵を前記認証代行サーバ装置から前記クライアント装置へ配送する手順と、

前記クライアント装置において前記サービスプロバイダ装置へ送信すべき情報を前記認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手順と、

前記クライアント装置から受け取った暗号化された情報を前記認証代行サーバ装置から前記サービスプロバイダ装置へ転送する手順と、

前記サービスプロバイダ装置において前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手順とを有し、認証代行サーバ装置には漏洩することなく、クライアント装置からサービスプロバイダ装置への情報転送を行うことを特徴とする認証代行方法。

【請求項2】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられた認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行方法において、

サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置に対して、前記クライアント装置の暗号用公開鍵を前記認証代行サーバ装置から配送する手順と、

前記サービスプロバイダ装置において前記クライアント装置へ送信すべき情報を前記認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手順と、

前記サービスプロバイダ装置から受け取った暗号化された情報を前記認証代行サーバ装置から前記クライアント装置へ転送する手順と、

前記クライアント装置において前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手順とを有し、認証代行サーバ装置には漏洩することなく、サービスプロバイダ装置からクライアント装置への情報転送を行うことを特徴とする認証代行方法。

【請求項3】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられた認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行方法において、

サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置の暗号用公開鍵を前記認証代行サーバ装置から前記クライアント装置へ配送する手順と、

前記クライアント装置において前記サービスプロバイダ装置との間の暗号通信用セッションキーあるいはこのセッションキーの元となるデータを生成し、前記セッションキーあるいはデータを前記認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手順と、

前記クライアント装置から受け取った暗号化された情報を前記認証代行サーバ装置から前記サービスプロバイダ装置へ転送する手順と、

前記サービスプロバイダ装置において前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して前記セッションキーを取得し、あるいは暗号用秘密鍵を用いた復号化により前記データを取得して、このデータから前記セッションキーを生成する手順と、

前記クライアント装置あるいは前記サービスプロバイダ装置において送信すべき情報を前記セッションキーを用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手順と、

前記セッションキーを用いて暗号化された情報を前記認証代行サーバ装置から前記サービスプロバイダ装置あるいは前記クライアント装置へ転送する手順と、

前記セッションキーを用いて暗号化された情報を前記サービスプロバイダ装置あるいは前記クライアント装置において自身が有する前記セッションキーを用いて復号化する手順とを有し、認証代行サーバ装置には漏洩することなく、クライアント装置とサービスプロバイダ装置間の双方向の情報転送を行うことを特徴とする認証代行方法。

【請求項4】　請求項1または3記載の認証代行方法において、

前記暗号用公開鍵を前記認証代行サーバ装置から前記クライアント装置へ配送する際に、前記暗号用公開鍵と共に暗号用公開鍵証明書を配送する手順と、

前記クライアント装置において前記暗号用公開鍵を用いた暗号化を行う前に、前記認証代行サーバ装置から受け取った暗号用公開鍵証明書を基に前記暗号用公開鍵を検証する手順とを有することを特徴とする認証代行方法。

【請求項5】　請求項1または3記載の認証代行方法において、

前記クライアント装置において暗号化を行う際に、このクライアント装置の認証情報を前記暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手順と、

前記サービスプロバイダ装置において復号化を行う際に、前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して前記認証情報を取得し、この認証情報を基に前記クライアント装置の

認証を行う手順とを有することを特徴とする認証代行方法。

【請求項６】　サービスを提供するサービスプロバイダ装置と、前記サービスプロバイダ装置と接続された、サービス提供を受けるクライアント装置と、前記サービスプロバイダ装置とクライアント装置との間に設けられた認証代行サーバ装置とからなり、前記認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サービスシステムにおいて、

前記認証代行サーバ装置は、サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置の暗号用公開鍵を前記クライアント装置へ配送し、前記クライアント装置から受け取った暗号化された情報を前記サービスプロバイダ装置へ転送する手段を有し、

前記クライアント装置は、前記サービスプロバイダ装置へ送信すべき情報を前記認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手段を有し、

前記サービスプロバイダ装置は、前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手段を有し、認証代行サーバ装置には漏洩することなく、クライアント装置からサービスプロバイダ装置への情報転送を行うことを特徴とする認証代行サービスシステム。

【請求項７】　サービスを提供するサービスプロバイダ装置と、前記サービスプロバイダ装置と接続された、サービス提供を受けるクライアント装置と、前記サービスプロバイダ装置とクライアント装置との間に設けられた認証代行サーバ装置とからなり、前記認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サービスシステムにおいて、

前記認証代行サーバ装置は、サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置に対して、前記クライアント装置の暗号用公開鍵を配送し、前記サービスプロバイダ装置から受け取った暗号化された情報を前記クライアント装置へ転送する手段を有し、

前記サービスプロバイダ装置は、前記クライアント装置へ送信すべき情報を前記認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手段を有し、

前記クライアント装置は、前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手段を有し、認証代行サーバ装置には漏洩することなく、サービスプロバイダ装置からクライアント装置への情報転送を行うことを特徴とする認証代行サービスシステム。

【請求項８】　サービスを提供するサービスプロバイダ装置と、前記サービスプロバイダ装置と接続された、サービス提供を受けるクライアント装置と、前記サービスプロバイダ装置とクライアント装置との間に設けられた認証代行サーバ装置とからなり、前記認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サービスシステムにおいて、

前記認証代行サーバ装置は、サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置の暗号用公開鍵を前記クライアント装置へ配送し、前記クライアント装置から受け取った暗号化された情報を前記サービスプロバイダ装置へ転送し、前記サービスプロバイダ装置から受け取った暗号化された情報を前記クライアント装置へ転送する手段を有し、

前記クライアント装置は、前記サービスプロバイダ装置との間の暗号通信用セッションキーあるいはこのセッションキーの元となるデータを生成し、前記セッションキーあるいはデータを前記認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信した後、前記サービスプロバイダ装置へ送信すべき情報を前記セッションキーを用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手段を有し、

前記サービスプロバイダ装置は、前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して前記セッションキーを取得し、あるいは暗号用秘密鍵を用いた復号化により前記データを取得して、このデータから前記セッションキーを生成した後、前記クライアント装置へ送信すべき情報を前記セッションキーを用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手段を有し、認証代行サーバ装置には漏洩することなく、クライアント装置とサービスプロバイダ装置間の双方向の情報転送を行うことを特徴とする認証代行サービスシステム。

【請求項９】　請求項６または８記載の認証代行サービスシステムにおいて、

前記認証代行サーバ装置は、前記暗号用公開鍵を前記クライアント装置へ配送する際に、前記暗号用公開鍵と共に暗号用公開鍵証明書を配送する手段を有し、

前記クライアント装置は、前記暗号用公開鍵を用いた暗号化を行う前に、前記認証代行サーバ装置から受け取った暗号用公開鍵証明書を基に前記暗号用公開鍵を検証する手段を有することを特徴とする認証代行サービスシステム。

【請求項１０】　請求項６または８記載の認証代行サービスシステムにおいて、

前記クライアント装置は、前記暗号化を行う際に、自装置の認証情報を前記暗号用公開鍵を用いて暗号化し、この暗号化された情報を前記認証代行サーバ装置へ送信する手段を有し、

前記サービスプロバイダ装置は、前記復号化を行う際

に、前記認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して前記認証情報を取得し、この認証情報を基に前記クライアント装置の認証を行う手段を有することを特徴とする認証代行サービスシステム。

【請求項１１】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられ、前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サーバ装置において、

前記認証代行サーバ装置は、サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置の暗号用公開鍵を前記クライアント装置へ配送し、この暗号用公開鍵を用いて暗号化された情報を前記クライアント装置から受け取り、暗号用秘密鍵を用いた復号化を行わせるべく、前記暗号化された情報を前記サービスプロバイダ装置へ転送する手段を有することを特徴とする認証代行サーバ装置。

【請求項１２】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられ、前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サーバ装置において、

前記認証代行サーバ装置は、サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置に対して、前記クライアント装置の暗号用公開鍵を配送し、この暗号用公開鍵を用いて暗号化された情報を前記サービスプロバイダ装置から受け取り、暗号用秘密鍵を用いた復号化を行わせるべく、前記暗号化された情報を前記クライアント装置へ転送する手段を有することを特徴とする認証代行サーバ装置。

【請求項１３】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられ、前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サーバ装置において、

前記認証代行サーバ装置は、サービス提供時、所望のサービスに対応した前記サービスプロバイダ装置の暗号用公開鍵を前記クライアント装置へ配送し、この暗号用公開鍵を用いて暗号化された暗号通信用セッションキーあるいはこのセッションキーの元となるデータを前記クライアント装置から受け取り、暗号用秘密鍵を用いた復号化を行わせるべく、前記暗号化されたセッションキーあるいはデータを前記サービスプロバイダ装置へ転送した後、前記セッションキーを用いて暗号化された、前記クライアント装置からの情報を前記サービスプロバイダ装置へ転送すると共に、前記セッションキーを用いて暗号化された、前記サービスプロバイダ装置からの情報を前記クライアント装置へ転送する手段を有することを特徴とする認証代行サーバ装置。

【請求項１４】　請求項１１または１３記載の認証代行サーバ装置において、

前記認証代行サーバ装置は、前記クライアント装置に前記暗号用公開鍵の検証を行わせるべく、前記暗号用公開鍵と共に暗号用公開鍵証明書を前記クライアント装置へ配送する手段を有することを特徴とする認証代行サーバ装置。

【請求項１５】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられた認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サービスシステムにおける前記クライアント装置であって、

前記認証代行サーバ装置からクライアント認証を受けるための署名を生成する署名生成手段を備えたＩＣカードからなると共に、

前記サービスプロバイダ装置へ送信すべき情報を暗号用公開鍵を用いて暗号化する暗号化手段と、前記ＩＣカードによって生成された署名を前記認証代行サーバ装置へ送信し、前記認証代行サーバ装置から送信された暗号用公開鍵を受け取って前記暗号化手段へ出力し、前記暗号化手段によって暗号化された情報を前記認証代行サーバ装置へ送信する送受信手段とを備えた処理装置からなることを特徴とするクライアント装置。

【請求項１６】　サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられた認証代行サーバ装置が前記クライアント装置に代わって前記サービスプロバイダ装置から認証を受ける認証代行サービスシステムにおける前記クライアント装置であって、

前記認証代行サーバ装置からクライアント認証を受けるための署名を生成する署名生成手段と、前記サービスプロバイダ装置へ送信すべき情報を暗号用公開鍵を用いて暗号化する暗号化手段とを備えたＩＣカードからなると共に、

前記ＩＣカードによって生成された署名を前記認証代行サーバ装置へ送信し、前記認証代行サーバ装置から送信された暗号用公開鍵を受け取って前記ＩＣカードへ出力し、前記ＩＣカードによって暗号化された情報を前記認証代行サーバ装置へ送信する送受信手段とを備えた処理装置からなることを特徴とするクライアント装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、サービスプロバイダ装置とクライアント装置との間に設けられた認証代行サーバ装置がクライアント装置に代わってサービスプロバイダ装置から認証を受ける認証代行方法、認証代行サービスシステム、認証代行サーバ装置及びクライアント装置に関するものである。

【０００２】

【従来の技術】従来、ネットワークによるサービス提供においては、秘密情報を用いてクライアント認証を行うことが一般的に行われている。ここで、秘密情報とは、例えばパスワード、ＲＳＡ（Ｒivest、Ｓhamir and Adleman ）などの公開鍵暗号方式における秘密鍵、ＤＥＳ（Ｄata Ｅncryption Ｓtandard）などの共有鍵方式の共有鍵を指す。クライアント認証を行う場合、一般的には、異なるサービス提供者に対しては、秘密情報は異なるものが使われる。

【０００３】例えば、図１３に示すように、あるクライアント装置（以下、クライアントと略する）Ｃがサービスプロバイダ装置（以下、サービスプロバイダと略する）ＳＰ－Ａによって提供されるサービスＡとサービスプロバイダＳＰ－Ｂによって提供されるサービスＢにそれぞれアクセスする際には、それぞれ別の秘密情報ＳｋＵ－ＡとＳｋＵ－Ｂを使用してクライアント認証を受ける必要がある。図１３において、ＣｅｒｔＵ－Ａ，ＣｅｒｔＵ－Ｂは、それぞれ秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂに対応した証明書である。この証明書は方式によっては不要である。例えば、公開鍵暗号方式では、秘密情報ＳｋＵは秘密鍵、ＣｅｒｔＵは公開鍵証明書となる。なお、ここでの「サービスプロバイダ」とは、現実の世界におけるサービス提供者（例えば企業）を必ずしも意味しない。つまり、現実の世界におけるサービス提供者が同じであっても、「サービスプロバイダが異なる」場合が有り得る。例えば、ある銀行の残高照会サービスと投資信託申込サービスは別のサービスプロバイダによって提供されるサービスと考える。

【０００４】異なるサービスプロバイダ間でクライアント情報の共有に同意すれば、秘密情報を同一にすることは可能である。例えば、図１３に示した例で言えば、サービスプロバイダＳＰ－ＡとＳＰ－Ｂが合意すれば、サービスプロバイダＳＰ－Ａに対する秘密情報ＳｋＵ－Ａを用いてサービスＢの提供を受けることは可能である（図１４）。特に、前述の例で同一銀行の２つのサービスであれば、現実の世界ではサービスプロバイダＳＰ－ＡとＳＰ－Ｂは同一であるため、合意は比較的容易である。しかし、存在するあらゆるサービスプロバイダ間で合意することは困難であり現実的ではない。クライアントＣに秘密情報を発行する際の方針の違いや、秘密情報の強度の違い、サービスの要求セキュリティの違いなどにより、合意が難しいケースは数多く存在する。つまり、クライアント認証に関する各サービスプロバイダの方針が異なるため、合意が難しい場合が数多く存在する。

【０００５】クライアント認証に関する方針がある程度一致する場合には、認証局を階層的に構成することにより、同一の秘密情報により認証を受けることが可能な場合もある。例えば、図１５に示すように、秘密情報に対する証明書を認証局ＣＡ－ＡあるいはＣＡ－Ｂが発行し、その認証局ＣＡ－Ａ，ＣＡ－Ｂの秘密情報に対してさらに上位の認証局ＣＡ－Ｒが証明書を発行する、というような形で認証ツリーを構成する。そして、サービスプロバイダＳＰ－Ａの秘密情報に対する認証ツリーとサービスプロバイダＳＰ－Ｂの秘密情報に対する認証ツリーが上位において交点を持っていれば、秘密情報ＳｋＵ－ＡによってサービスプロバイダＳＰ－Ｂがサービスを提供できる場合がある。図１５において、ＣＡ－Ａ，ＣＡ－ＢはサービスプロバイダＳＰ－Ａのサービスを受けるための認証局、ＣＡ－Ｒは認証局ＣＡ－Ａ，ＣＡ－Ｂの上位の認証局である。なお、ＣＡ－Ａ，ＣＡ－ＢとＣＡ－Ｒとの中間、あるいはＣＡ－Ｒの上位に他の認証局が介在する場合もある。サービスプロバイダＳＰ－Ｂは、自クライアントの認証局であるＣＡ－Ｂの上位認証局ＣＡ－Ｒが認証しているＣＡ－Ａの発行した証明書により、秘密情報ＳｋＵ－Ａを用いたクライアント認証を認める。

【０００６】図１５の場合においても、あらゆるサービスの認証ツリーに交点を持たせることは困難であり、また、交点があったとしても、セキュリティの方針の違いなどにより必ずしもサービス提供が可能とは限らない。つまり、クライアントＣが誰であるか分かったとしても、サービスプロバイダの方針によってはサービス提供を拒否する場合があり得る。したがって、「クライアント認証が必要な複数のサービスを受ける場合、クライアントは、各サービスに対応した複数の秘密情報を管理する必要がある」、ということが一般的には言える。ここでは、同一の秘密情報により認証を受けることができる場合を「サービスの認証体系が同一」と呼ぶこととする。反対に、同一の秘密情報により認証を受けることができない場合を「サービスの認証体系が異なる」と呼ぶこととする。

【０００７】一般に、秘密情報の管理機能、及び秘密情報を用いてクライアント認証を受ける機能をクライアントＣに実装するコストは大きく、複数のサービスに対して複数の秘密情報を用いる場合には更に大きくなる。秘密情報の管理に関して言えば、秘密情報を遺失した場合にはサービスを受けられなくなってしまうという問題が生じ、秘密情報が漏洩した場合には他のクライアントが自クライアントになりすます危険があるため、遺失防止機能及び漏洩防止機能の実装のコストが大きくなる。複数の秘密情報の管理が必要な場合には、管理そのもののコストが大きくなる上に、管理形態によっては、どれか一つの秘密情報が遺失・漏洩すると他の秘密情報も再発行しなければならない場合があり、再発行コストが大きくなる。

【０００８】秘密情報を用いたクライアント認証機能に関しては、例えば公開鍵暗号方式を用いる場合、秘密鍵の管理以外に、対応する公開鍵証明書の保管機能、公開鍵証明書のサービスプロバイダへの送信機能、秘密情報

（公開鍵暗号方式における鍵ペアなど）の生成機能、認証局への秘密情報の登録機能、公開鍵証明書取得機能などがクライアントCに必要になる。クライアントCに簡易な端末、例えばセットトップボックスなどを想定した場合、管理する秘密情報が少なかったとしてもこれら全ての機能を実装するコストは大きいが、秘密情報が増えるとさらに大きくなる。こうしたことから、クライアントCで管理する秘密情報の数はできるだけ少なくしたいという、クライアント管理者の要求が存在する。

【０００９】このようなクライアント管理者の要求、すなわち認証体系が異なる複数のサービスを受ける場合に、クライアント管理者が管理する秘密情報を少なくしたいということを解決する従来技術としては以下のような３つがある。

従来技術１：認証局同士の相互認証。

従来技術２：認証代行サーバへ秘密情報を預ける形態での認証処理の委託。

従来技術３：認証代行サーバ自身の秘密情報を使う形態での認証処理の委託。

【００１０】従来技術１は、図１６に示すように、認証ツリーに交点を持たない場合や、持っていたとしても当該サービス提供可能なレベルで各ＳＰの認証に関する方針が一致していなかった場合に、認証局ＣＡ－Ａ０，ＣＡ－Ｂ０同士の相互認証書を確認することで、同一の秘密情報により認証を受けることができるようにする方式である。図１６において、ＣＡ－Ａ１，ＣＡ－Ａ２，ＣＡ－Ｂ１，ＣＡ－Ｂ２は認証局、ＣＡ－Ａ０は認証局ＣＡ－Ａ１，ＣＡ－Ａ２の上位の認証局、ＣＡ－Ｂ０は認証局ＣＡ－Ｂ１，ＣＡ－Ｂ２の上位の認証局である。サービスプロバイダＳＰ－Ｂは、自クライアントの認証局（例えばＣＡ－Ｂ１）の上位認証局ＣＡ－Ｂ０と他の上位認証局ＣＡ－Ａ０との間で相互認証書が存在することにより、秘密情報ＳｋＵ－Ａを用いたクライアント認証を認める。この従来技術１は有望な方式の一つではある。しかし、サービスプロバイダや認証局に大きな機能追加が必要であり、また相互認証書を発行するということは結局各サービスプロバイダの合意形成が必要であることから、適用範囲が限られる。したがって、本発明では考慮の対象としない。

【００１１】従来技術２は、図１７に示すように、クライアントＣが所属する一つの認証体系内にその他の認証体系での秘密情報、証明書、ＣＲＬ（失効証明書リスト）などを管理する認証代行サーバＳを設け、クライアント認証が必要なサービスについては認証代行サーバＳと各サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ間で認証を行う方式である。図１７において、ＳｋＵ－Ｐは認証代行サーバＳとクライアントＣ間の認証に用いるための秘密情報である。この秘密情報ＳｋＵ－Ｐについては、クライアント管理者が記憶して、クライアントＣ自体では管理しない場合もある。また、ＣｅｒｔＵ－Ｐは、秘密情報ＳｋＵ－Ｐに対応した証明書である。この証明書は方式によっては不要である。例えば、公開鍵暗号方式では、秘密情報ＳｋＵ－Ｐは秘密鍵、ＣｅｒｔＵ－Ｐは公開鍵証明書となる。

【００１２】従来技術２は、従来技術１と比べて認証局、サービスプロバイダ側には変更が少ないという利点がある。認証局及びサービスプロバイダ側から見ると、認証代行サーバＳは意識されず、クライアントＣとして認証される。例えば、インターネット上のクレジット決済や銀行口座決済を実現する方式であるＳＥＴ（Secure Electronic Transaction ）やＳＥＣＥ（Secure Electronic Commerce Environment）においては利用者認証が必要となり、複数のクレジット会社及び銀行からサービスを受けるために、それぞれ秘密情報を保持する必要があるが、この秘密情報をサーバウォレットと呼ばれる認証代行サーバに預ける方式が提案されており、一部製品化されている。

【００１３】従来技術３は、図１８に示すように、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからクライアント認証を受ける際に、各クライアントＣの秘密情報を用いるのではなく、認証代行サーバＳ自身の秘密情報ＳｋＰを用いる方式である。図１８において、ＣｅｒｔＰは秘密情報ＳｋＰに対応した証明書である。つまり、サービスプロバイダ側からは、認証代行サーバＳがサービスを受けているように見える。この従来技術３では、従来技術２と同様に、各クライアントＣは各サービスに対応する秘密情報を管理する必要はなく、また認証代行サーバＳにおいても、自身の秘密情報のみを管理すればよいことになる。

【００１４】

【発明が解決しようとする課題】しかしながら、以上の従来技術２、従来技術３には、以下のような３つの問題点があった。

問題点１：クライアントＣとサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ間でやりとりする全ての情報が認証代行サーバＳに漏洩する。クライアントＣにとって認証代行サーバＳは信頼できる主体であるが、サービスによってはサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂとやりとりする情報を秘匿したい場合がある。仮に、クライアントＣと認証代行サーバＳの間、認証代行サーバＳとサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂの間をそれぞれ暗号化していたとしても、認証代行サーバＳ内では情報が復号化されるため、情報が漏洩する恐れがある。なお、この問題点１は、従来技術２、従来技術３の両者に共通するものである。

【００１５】問題点２：認証代行サーバＳがクライアントＣになりすました場合、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ側では確認できない。従来技術２において、認証代行サーバＳは、クライアント秘密情報を保持しているため、クライアントＣになりすますことが可能

である。認証代行サーバSは、一般には利用者からもサービスプロバイダSP－A，SP－Bからも信頼できる主体であるが、例えば、万が一、認証代行サーバSのシステム運用者などが不正を働いた場合や、クライアント利用者がサービスの提供を受けたことを否認した場合などを想定すると、サービスプロバイダSP－A，SP－B側で直接クライアントを認証できる手段を用意しておくことが望ましい。もちろん、認証代行サーバSが存在することの利点を考えると、その際の認証手段は認証代行サーバSが存在しない場合に比べて簡易である必要がある。

【００１６】問題点３：クライアントCとサービスプロバイダSP－A，SP－B間でサービスを提供する責任、及びサービス対価を回収する責任が認証代行サーバSに生じやすい。従来技術３において、サービスプロバイダSP－A，SP－Bは、認証代行サーバS自身の秘密情報によりクライアントを認証しサービス提供を行う。つまり、サービスプロバイダSP－A，SP－Bは、認証代行サーバSを意識してサービスを提供しているのであり、そのサービスをクライアントCに届ける責任と、サービス対価をクライアントCから徴収する責任が認証代行サーバSに生じやすい（実際に生じるかどうかは当事者間の契約や法体系による）。その場合、責任が大きくなればなるほど、認証代行サーバSを運営できる主体が限られてしまうことになる。本発明は、上記課題を解決するためになされたもので、認証に関するクライアントの負担を認証代行サーバにより解決しつつ、前記問題点１、問題点２及び問題点３を解消することができる認証代行方法、認証代行サービスシステム、認証代行サーバ装置及びクライアント装置を提供することを目的とする。

【００１７】

【課題を解決するための手段】本発明の認証代行方法は、サービスを提供するサービスプロバイダ装置とサービス提供を受けるクライアント装置との間に設けられた認証代行サーバ装置がクライアント装置に代わってサービスプロバイダ装置から認証を受けるようにしたものである。そして、本発明の認証代行方法は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵を認証代行サーバ装置からクライアント装置へ配送する手順と、クライアント装置においてサービスプロバイダ装置へ送信すべき情報を認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手順と、クライアント装置から受け取った暗号化された情報を認証代行サーバ装置からサービスプロバイダ装置へ転送する手順と、サービスプロバイダ装置において認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手順とを有するものである。また、本発明の認証代行方法は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置に対して、クライアント装置の暗号用公開鍵を認証代行サーバ装置から配送する手順と、サービスプロバイダ装置においてクライアント装置へ送信すべき情報を認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手順と、サービスプロバイダ装置から受け取った暗号化された情報を認証代行サーバ装置からクライアント装置へ転送する手順と、クライアント装置において認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手順とを有するものである。

【００１８】また、本発明の認証代行方法は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵を認証代行サーバ装置からクライアント装置へ配送する手順と、クライアント装置においてサービスプロバイダ装置との間の暗号通信用セッションキーあるいはこのセッションキーの元となるデータを生成し、セッションキーあるいはデータを認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手順と、クライアント装置から受け取った暗号化された情報を認証代行サーバ装置からサービスプロバイダ装置へ転送する手順と、サービスプロバイダ装置において認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化してセッションキーを取得し、あるいは暗号用秘密鍵を用いた復号化によりデータを取得して、このデータからセッションキーを生成する手順と、クライアント装置あるいはサービスプロバイダ装置において送信すべき情報をセッションキーを用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手順と、セッションキーを用いて暗号化された情報を認証代行サーバ装置からサービスプロバイダ装置あるいはクライアント装置へ転送する手順と、セッションキーを用いて暗号化された情報をサービスプロバイダ装置あるいはクライアント装置において自身が有するセッションキーを用いて復号化する手順とを有するものである。

【００１９】また、本発明の認証代行方法の１構成例として、暗号用公開鍵を認証代行サーバ装置からクライアント装置へ配送する際に、暗号用公開鍵と共に暗号用公開鍵証明書を配送する手順と、クライアント装置において暗号用公開鍵を用いた暗号化を行う前に、認証代行サーバ装置から受け取った暗号用公開鍵証明書を基に暗号用公開鍵を検証する手順とを有するものである。また、本発明の認証代行方法の１構成例として、クライアント装置において暗号化を行う際に、このクライアント装置の認証情報を暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手順と、サービスプロバイダ装置において復号化を行う際に、認

証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して認証情報を取得し、この認証情報を基にクライアント装置の認証を行う手順とを有するものである。

【００２０】また、本発明の認証代行サービスシステムとして、認証代行サーバ装置（Ｓ）は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵をクライアント装置へ配送し、クライアント装置から受け取った暗号化された情報をサービスプロバイダ装置へ転送する手段を有し、クライアント装置（Ｃ）は、サービスプロバイダ装置へ送信すべき情報を認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手段を有し、サービスプロバイダ装置（ＳＰ－Ａ，ＳＰ－Ｂ）は、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手段を有するものである。また、本発明の認証代行サービスシステムとして、認証代行サーバ装置（Ｓ）は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置に対して、クライアント装置の暗号用公開鍵を配送し、サービスプロバイダ装置から受け取った暗号化された情報をクライアント装置へ転送する手段を有し、サービスプロバイダ装置（ＳＰ－Ａ，ＳＰ－Ｂ）は、クライアント装置へ送信すべき情報を認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手段を有し、クライアント装置（Ｃ）は、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化する手段を有するものである。

【００２１】また、本発明の認証代行サービスシステムとして、認証代行サーバ装置（Ｓ）は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵をクライアント装置へ配送し、クライアント装置から受け取った暗号化された情報をサービスプロバイダ装置へ転送し、サービスプロバイダ装置から受け取った暗号化された情報をクライアント装置へ転送する手段を有し、クライアント装置（Ｃ）は、サービスプロバイダ装置との間の暗号通信用セッションキーあるいはこのセッションキーの元となるデータを生成し、セッションキーあるいはデータを認証代行サーバ装置から受け取った暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信した後、サービスプロバイダ装置へ送信すべき情報をセッションキーを用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手段を有し、サービスプロバイダ装置（ＳＰ－Ａ，ＳＰ－Ｂ）は、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化してセッションキーを取得し、あるいは暗号用秘密鍵を用いた復号化によりデータを取得して、このデータからセッションキーを生成した後、クライアント装置へ送信すべき情報をセッションキーを用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手段を有するものである。

【００２２】また、本発明の認証代行サービスシステムの１構成例として、認証代行サーバ装置は、暗号用公開鍵をクライアント装置へ配送する際に、暗号用公開鍵と共に暗号用公開鍵証明書を配送する手段を有し、クライアント装置は、暗号用公開鍵を用いた暗号化を行う前に、認証代行サーバ装置から受け取った暗号用公開鍵証明書を基に暗号用公開鍵を検証する手段を有するものである。また、本発明の認証代行サービスシステムの１構成例として、クライアント装置は、暗号化を行う際に、自装置の認証情報を暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信する手段を有し、サービスプロバイダ装置は、復号化を行う際に、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して認証情報を取得し、この認証情報を基にクライアント装置の認証を行う手段を有するものである。

【００２３】また、本発明の認証代行サーバ装置（Ｓ）は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵をクライアント装置へ配送し、この暗号用公開鍵を用いて暗号化された情報をクライアント装置から受け取り、暗号用秘密鍵を用いた復号化を行わせるべく、暗号化された情報をサービスプロバイダ装置へ転送する手段を有するものである。また、本発明の認証代行サーバ装置（Ｓ）は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置に対して、クライアント装置の暗号用公開鍵を配送し、この暗号用公開鍵を用いて暗号化された情報をサービスプロバイダ装置から受け取り、暗号用秘密鍵を用いた復号化を行わせるべく、暗号化された情報をクライアント装置へ転送する手段を有するものである。

【００２４】また、本発明の認証代行サーバ装置（Ｓ）は、サービス提供時、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵をクライアント装置へ配送し、この暗号用公開鍵を用いて暗号化された暗号通信用セッションキーあるいはこのセッションキーの元となるデータをクライアント装置から受け取り、暗号用秘密鍵を用いた復号化を行わせるべく、暗号化されたセッションキーあるいはデータをサービスプロバイダ装置へ転送した後、セッションキーを用いて暗号化された、クライアント装置からの情報をサービスプロバイダ装置へ転送すると共に、セッションキーを用いて暗号化された、サービスプロバイダ装置からの情報をクライアント装置へ転送する手段を有するものである。また、本発明の認証代行サーバ装置の１構成例は、クライアント装置に暗号用公開鍵の検証を行わせるべく、暗号用公開鍵と共に暗号用公開鍵証明書をクライアント装置へ配送する手段を有するものである。

【００２５】また、本発明のクライアント装置（Ｃ）は、認証代行サーバ装置からクライアント認証を受けるための署名を生成する署名生成手段を備えたＩＣカードからなると共に、サービスプロバイダ装置へ送信すべき情報を暗号用公開鍵を用いて暗号化する暗号化手段と、ＩＣカードによって生成された署名を認証代行サーバ装置へ送信し、認証代行サーバ装置から送信された暗号用公開鍵を受け取って暗号化手段へ出力し、暗号化手段によって暗号化された情報を認証代行サーバ装置へ送信する送受信手段とを備えた処理装置からなるものである。また、本発明のクライアント装置（Ｃ）は、認証代行サーバ装置からクライアント認証を受けるための署名を生成する署名生成手段と、サービスプロバイダ装置へ送信すべき情報を暗号用公開鍵を用いて暗号化する暗号化手段とを備えたＩＣカードからなると共に、ＩＣカードによって生成された署名を認証代行サーバ装置へ送信し、認証代行サーバ装置から送信された暗号用公開鍵を受け取ってＩＣカードへ出力し、ＩＣカードによって暗号化された情報を認証代行サーバ装置へ送信する送受信手段とを備えた処理装置からなるものである。

【００２６】

【発明の実施の形態】［実施の形態の１］次に、本発明の実施の形態について図面を参照して詳細に説明する。図１は本発明の第１の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。本実施の形態の認証代行サービスシステムは、前述の従来技術２あるいは従来技術３において、認証代行サーバ装置（以下、認証代行サーバと略する）Ｓが複数のサービスプロバイダ装置（以下、サービスプロバイダと略する）ＳＰ－Ａ，ＳＰ－Ｂの公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂをクライアント装置（以下、クライアントと略する）Ｃにサービス提供時に配送し、認証代行サーバＳには秘匿しておきたい情報をこの公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂを用いてクライアントＣ側で暗号化させて認証代行サーバＳに返却させ、この情報を認証代行サーバＳがサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに送信し、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂで秘密鍵ＳｋＳＰ－Ａ，ＳｋＳＰ－Ｂによって復号化させることで、認証代行サーバＳには漏洩することなく、クライアントＣからサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへの情報転送を実現するものである。

【００２７】サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂとクライアントは、ネットワークを介して接続され、このネットワークの途中に認証代行サーバ装置Ｓが設けられている。図１において、ＰｋＳＰ－Ａ，ＰｋＳＰ－ＢはそれぞれサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂの暗号用公開鍵、ＳｋＳＰ－Ａ，ＳｋＳＰ－Ｂそれぞれサービスプロバイダ ＳＰ－Ａ，ＳＰ－Ｂの暗号用秘密鍵である。また、ＳｋＵ－Ａ，ＳｋＵ－ＢはそれぞれサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからサービスを受けるための秘密情報、ＳｋＰは認証代行サーバＳ自身の秘密情報である。本実施の形態のシステムが従来技術２に対応する方式の場合には、秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂを用いてクライアントＣの認証が行われ、従来技術３に対応する方式の場合には、秘密情報ＳｋＰを用いてクライアントＣの認証が行われる。

【００２８】次に、このような認証代行サービスシステムの動作を説明する。サービス提供時、認証代行サーバＳは、クライアントＣが要求するサービスに応じて適切なサービスプロバイダＳＰ－Ａの暗号用公開鍵ＰｋＳＰ－Ａをクライアント Ｃに配送すると共に、この公開鍵ＰｋＳＰ－Ａを使った情報の暗号化要求、秘匿情報に関連したその他情報変換要求、暗号化された情報及び変換された情報の返却要求をクライアントＣに対して行う。

【００２９】ここで、秘匿情報に関連したその他情報変換要求とは、秘匿情報をサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂでも復号化できない形態へ変換する処理の要求であり、サービスにより必要な場合のみ出されるもので、例えば一方向ハッシュ演算を指す。

【００３０】クライアントＣは、認証代行サーバＳの要求に応じて、サービスプロバイダＳＰ－Ａへ送信すべき情報を公開鍵ＰｋＳＰ－Ａを用いて暗号化し、暗号化した情報を認証代行サーバＳに送信する。また、クライアントＣは、秘匿情報に関連したその他情報変換要求がなされた場合、ハッシュ演算等の変換を行った情報を暗号化した情報と共に認証代行サーバＳに送信する。

【００３１】認証代行サーバＳは、クライアントＣから送信された情報を受け取り、この情報をサービスプロバイダＳＰ－Ａへ転送すると共に、サービスプロバイダＳＰ－Ａに対して復号化要求を行う。サービスプロバイダＳＰ－Ａは、認証代行サーバＳから送信された情報を受け取り、この情報を自身が有する秘密鍵ＳｋＳＰ－Ａを用いて復号化する。

【００３２】こうして、クライアントＣからサービスプロバイダＳＰ－Ａへの情報が認証代行サーバＳに漏洩することを防止でき、前記問題点１の部分的な解決が可能になる。なお、以上の動作説明では、サービス提供がサービスプロバイダＳＰ－Ａによって行われる場合について説明しているが、サービス提供がサービスプロバイダＳＰ－Ｂによって行われる場合には、公開鍵ＰｋＳＰ－Ａの代わりにＰｋＳＰ－Ｂが用いられ、クライアントＣからの情報がサービスプロバイダＳＰ－Ｂに転送され、サービスプロバイダＳＰ－Ｂが秘密鍵ＳｋＳＰ－Ｂを用いて情報を復号化する。

【００３３】また、前記暗号化要求、秘匿情報に関連したその他情報変換要求、暗号化された情報及び変換された情報の返却要求は、クライアントＣが自律的に行うことで省略することができ、同様に前記復号化要求は、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂが自律的に行うことで省略することができる。

【００３４】また、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからサービス提供を受けるためには、前述の従来技術２あるいは従来技術３で説明したように認証代行サーバＳがクライアントＣに代わってサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからクライアント認証を受ける処理（秘密情報ＳｋＵ－Ａ，ＳｋＵ－ＢあるいはＳｋＰによる署名の生成とこの署名のサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへの送信など）が必要である。この処理は、認証代行サーバＳによる公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂの配送からサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂによる情報の復号化に至る一連のシーケンスより前の時点、クライアントＣから受け取った情報をサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに配送する時点、あるいは前記一連のシーケンスより後の時点のいずれに行ってもよい。

【００３５】［実施の形態の２］図２は本発明の第２の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。本実施の形態の認証代行サービスシステムは、前述の従来技術２あるいは従来技術３において、認証代行サーバＳがクライアントＣの公開鍵ＰｋＵ’－Ａ，ＰｋＵ’－ＢをサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに配送し、認証代行サーバＳには秘匿しておきたい情報をこの公開鍵ＰｋＵ’－Ａ，ＰｋＵ’－Ｂを用いてサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ側で暗号化させて認証代行サーバＳに返却させ、この情報を認証代行サーバＳがクライアントＣに送信し、クライアントＣで秘密鍵ＳｋＵ’－Ａ，ＳｋＵ’－Ｂによって復号化させることで、認証代行サーバＳには漏洩することなく、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからクライアントへの情報転送を実現するものである。

【００３６】図２において、ＣｅｒｔＵ’－Ａ，ＣｅｒｔＵ’－ＢはそれぞれサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに対するクライアントＣの暗号用公開鍵証明書、ＰｋＵ’－Ａ，ＰｋＵ’－ＢはそれぞれサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに対するクライアントＣの暗号用公開鍵、ＳｋＵ’－Ａ，ＳｋＵ’－ＢはそれぞれサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに対するクライアントＣの暗号用秘密鍵である。本実施の形態のシステムが従来技術２に対応する方式の場合には、秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂを用いてクライアントＣの認証が行われ、従来技術３に対応する方式の場合には、秘密情報ＳｋＰを用いてクライアントＣの認証が行われる。

【００３７】次に、このような認証代行サービスシステムの動作を説明する。サービス提供時，認証代行サーバＳは、クライアントＣが要求するサービスに応じた適切なサービスプロバイダＳＰ－Ａに対して、クライアントＣの暗号用公開鍵ＰｋＵ’－Ａを暗号用公開鍵証明書ＣｅｒｔＵ’－Ａに付加する形で配送すると共に、この公開鍵ＰｋＵ’－Ａを使った情報の暗号化要求を行う。

【００３８】この認証代行サーバＳの要求により、サービスプロバイダＳＰ－Ａは、クライアントＣへ送信すべき情報を暗号用公開鍵証明書ＣｅｒｔＵ’－Ａに含まれる公開鍵ＰｋＵ’－Ａを用いて暗号化し、暗号化した情報を認証代行サーバＳに送信する。認証代行サーバＳは、サービスプロバイダＳＰ－Ａから送信された情報を受け取り、この情報をクライアントＣへ転送すると共に、クライアントＣに対して復号化要求を行う。

【００３９】クライアントＣは、認証代行サーバＳから送信された情報を受け取り、この情報を自身が有する秘密鍵ＳｋＵ’－Ａを用いて復号化する。こうして、サービスプロバイダＳＰ－Ａからクライアントへの情報が認証代行サーバＳに漏洩することを防止でき、前記問題点１の部分的な解決が可能になる。なお、以上の動作説明では、サービス提供がサービスプロバイダＳＰ－Ａによって行われる場合について説明しているが、サービス提供がサービスプロバイダＳＰ－Ｂによって行われる場合には、証明書ＣｅｒｔＵ’－Ａ、公開鍵ＰｋＵ’－Ａの代わりにそれぞれＣｅｒｔＵ’－Ｂ、ＰｋＵ’－Ｂが用いられ、サービスプロバイダＳＰ－Ｂからの情報がクライアントＣに転送され、クライアントＣが秘密鍵ＳｋＵ’－Ｂを用いて情報を復号化する。

【００４０】また、前記暗号化要求は、サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂが自律的に行うことで省略することができ、同様に前記復号化要求は、クライアントＣが自律的に行うことで省略することができる。本実施の形態では、秘密鍵ＳｋＵ’－Ａ，ＳｋＵ’－Ｂをクライアントで管理しなくてはならず、サービス毎に秘密鍵が必要になってしまう、ただし、秘密鍵ＳｋＵ’－Ａ，ＳｋＵ’－Ｂに対応する公開鍵証明書ＣｅｒｔＵ’－Ａ，ＣｅｒｔＵ’－Ｂの管理は認証代行サーバＳに委託することが可能である。そのため、認証代行サーバＳの有り／無しに関わらず、そもそも暗号用の秘密鍵が必要なサービスに対しての適用が有効である。

【００４１】また、認証代行サーバＳがクライアントＣに代わってサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからクライアント認証を受ける処理（秘密情報ＳｋＵ－Ａ，ＳｋＵ－ＢあるいはＳｋＰによる署名の生成とこの署名のサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへの送信など）は、認証代行サーバＳによる公開鍵ＰｋＵ’－Ａ，ＰｋＵ’－Ｂの配送からクライアントＣによる情報の復号化に至る一連のシーケンスより前の時点、あるいは前記一連のシーケンスより後の時点のいずれに行ってもよい。

【００４２】［実施の形態の３］図３は本発明の第３の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。本実施の形態の認証代行サービスシステムは、実施の形態の１において、暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－ＢのクライアントＣへの配送時に、セッションキーの生成あるいはセッションキーの元となるデータの生成をクライアントＣに対して要求し、

さらにこれらを暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂを用いて暗号化させた上で返却させ、暗号化された情報をサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへ転送することで、認証代行サーバＳには漏洩することなく、クライアントＣとサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ間の双方向の情報転送を実現するものである。

【００４３】図３において、ＳＳｋＡ，ＳＳｋＢはそれぞれクライアントＣとサービスプロバイダＳＰ－Ａ間、クライアントＣとサービスプロバイダＳＰ－Ｂ間の暗号通信用セッションキー、ＳｄＳＳＫＡ，ＳｄＳＳｋＢはそれぞれ暗号通信用セッションキーＳＳｋＡ，ＳＳｋＢの生成の元となる例えば乱数等のデータである。本実施の形態のシステムが従来技術２に対応する方式の場合には、秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂを用いてクライアントＣの認証が行われ、従来技術３に対応する方式の場合には、秘密情報ＳｋＰを用いてクライアントＣの認証が行われる。

【００４４】次に、このような認証代行サービスシステムの動作を説明する。サービス提供時、認証代行サーバＳは、クライアントＣが要求するサービスに応じて適切なサービスプロバイダＳＰ－Ａの暗号用公開鍵ＰｋＳＰ－Ａをクライアント Ｃに配送すると共に、暗号通信用セッションキーＳＳｋＡの生成要求あるいはセッションキーＳＳｋＡの元となるデータＳｄＳＳＫＡの生成要求、公開鍵ＰｋＳＰ－Ａを用いたセッションキーＳＳｋＡあるいはデータＳｄＳＳＫＡの暗号化要求、暗号化された情報の返却要求をクライアントＣに対して行う。

【００４５】この認証代行サーバＳの要求により、クライアントＣは、暗号通信用セッションキーＳＳｋＡを生成する。また、クライアントＣは、場合によってはセッションキーＳＳｋＡの元となるデータＳｄＳＳＫＡを生成する。そして、クライアントＣは、セッションキーＳＳｋＡあるいはデータＳｄＳＳＫＡを公開鍵ＰｋＳＰ－Ａを用いて暗号化し、暗号化した情報を認証代行サーバＳに送信する。

【００４６】認証代行サーバＳは、クライアントＣから送信された情報を受け取り、この情報をサービスプロバイダＳＰ－Ａへ転送すると共に、必要であればデータＳｄＳＳＫＡから暗号通信用セッションキーＳＳｋＡの生成をサービスプロバイダＳＰ－Ａに対して要求する。

【００４７】サービスプロバイダＳＰ－Ａは、認証代行サーバＳから送信された情報を受け取り、この情報を自身が有する秘密鍵ＳｋＳＰ－Ａを用いて復号化し、セッションキーＳＳｋＡを取得する。また、サービスプロバイダＳＰ－Ａは、認証代行サーバＳからセッションキーＳＳｋＡの生成を要求された場合、認証代行サーバＳから送信された情報を秘密鍵ＳｋＳＰ－Ａを用いて復号化して、データＳｄＳＳＫＡを取得して、このデータＳｄＳＳＫＡからセッションキーＳＳｋＡを生成する。

【００４８】以後、クライアントＣとサービスプロバイダＳＰ－Ａ間の双方向の通信について安全な情報のやりとりが可能となる。すなわち、クライアントＣからサービスプロバイダＳＰ－Ａへ情報を送信する場合、クライアントＣは、送信すべき情報をセッションキーＳＳｋＡを用いて暗号化した後に送信し、暗号化された情報を認証代行サーバＳを介して受け取ったサービスプロバイダＳＰ－Ａは、自身が有するセッションキーＳＳｋＡを用いて情報を復号化する。

【００４９】一方、サービスプロバイダＳＰ－Ａからクライアント Ｃへ情報を送信する場合、サービスプロバイダＳＰ－Ａは、送信すべき情報をセッションキーＳＳｋＡを用いて暗号化した後に送信し、暗号化された情報を認証代行サーバＳを介して受け取ったクライアントＣは、自身が有するセッションキーＳＳｋＡを用いて情報を復号化する。

【００５０】こうして、クライアントＣからサービスプロバイダＳＰ－Ａへの情報のみならず、サービスプロバイダＳＰ－Ａからクライアント Ｃへの情報配送においても、認証代行サーバＳに情報が漏洩することを防止することが可能になる。なお、以上の動作説明では、サービス提供がサービスプロバイダＳＰ－Ａによって行われる場合について説明しているが、サービス提供がサービスプロバイダＳＰ－Ｂによって行われる場合には、公開鍵ＰｋＳＰ－Ａ、セッションキーＳＳｋＡ、データＳｄＳＳＫＡの代わりにそれぞれＰｋＳＰ－Ｂ、セッションキーＳＳｋＢ、情報ＳｄＳＳＫＢが用いられ、クライアントＣからの情報がサービスプロバイダＳＰ－Ｂに転送され、サービスプロバイダＳＰ－ＢがデータＳｄＳＳＫＢからセッションキーＳＳｋＢを生成する。

【００５１】また、前記生成要求、暗号化要求、暗号化された情報の返却要求はクライアントＣが自律的に行うことで省略することができ、同様に前記生成要求はサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂが自律的に行うことで省略することができる。

【００５２】また、認証代行サーバＳがクライアントＣに代わってサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからクライアント認証を受ける処理（秘密情報ＳｋＵ－Ａ，ＳｋＵ－ＢあるいはＳｋＰによる署名の生成とこの署名のサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへの送信など）は、認証代行サーバＳによる公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂの配送からサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂによるセッションキーの生成に至る一連のシーケンスより前の時点、暗号化されたセッションキーＳＳｋＡ，ＳＳｋＢあるいはデータＳｄＳＳＫＡ，ＳｄＳＳｋＢをサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに配送する時点、あるいは前記一連のシーケンスより後の時点のいずれに行ってもよい。

【００５３】［実施の形態の４］図４は本発明の第４の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。実施の形態の１あるいは実施の形

態の3では、サービスプロバイダSP－A，SP－Bの暗号用公開鍵PkSP－A，PkSP－Bを誰がどのように検証するかという問題が存在する。例えば、認証代行サーバSに公開鍵PkSP－A，PkSP－Bの検証（例えば、公開鍵証明書の認証局署名の検証やCRLのチェックなど）を委託した場合には、以下のような問題が生じる。

【0054】すなわち、偽の公開鍵を認証代行サーバSからクライアントCに配送し、クライアントCからサービスプロバイダSP－A，SP－Bへの情報を認証代行サーバSが認知している、偽の公開鍵に対応する秘密鍵を用いて復号化した上で、この復号化した情報を改めて正しい公開鍵PkSP－A，PkSP－Bを用いて暗号化してサービスプロバイダSP－A，SP－Bへ送信するという操作を行えば、認証代行サーバSにおいて情報を不正に取得することが可能になる。

【0055】そこで、本実施の形態の認証代行サービスシステムは、サービスプロバイダSP－A，SP－Bの暗号用公開鍵PkSP－A，PkSP－Bの検証を認証代行サーバSからクライアントCに対して要求する。すなわち、認証代行サーバSは、暗号用公開鍵PkSP－A，PkSP－Bと共に、暗号用公開鍵証明書CertSP－A，CertSP－Bをクライアントへ配送する。

【0056】クライアントCは、例えば上位認証局の証明書をサービスプロバイダSP－A，SP－B毎に保持しており、認証代行サーバSから配送されてきた公開鍵証明書CertSP－A，CertSP－Bを上位認証局の証明書を用いて検証する。また、クライアントCは、公開鍵証明書CertSP－A，CertSP－Bが失効していないかどうかの確認を証明書取り消しリスト（Certificate Revocation List ，以下、CRLと略する）に基づいて行う。

【0057】こうして、暗号用公開鍵PkSP－A，PkSP－Bの検証を行うことができる。なお、認証代行サーバSはクライアントCにとっては十分に信頼でき、偽の公開鍵をクライアントCに配送することは考慮しなくてよい場合が多い。すなわち、一般には、クライアントCとサービスプロバイダSP－A，SP－B間の双方向の通信に係る情報漏洩については信頼しきれないが、偽の公開鍵配送については考慮しなくてよいという場合が多く、実施の形態の1あるいは3で十分である。

【0058】その理由は、認証代行サーバSの運用作業者や認証代行サーバSに不正にアクセスする外部侵入者にとっては、サーバS内で平文になる情報を盗む方が、偽の公開鍵配送による一連の不正行為を実施するよりも実行が容易だからである。また、前記検証要求は、クライアントCが公開鍵の検証を自律的に行うことで省略することができる。

【0059】［実施の形態の5］図5は本発明の第5の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。本実施の形態の認証代行サービスシステムは、実施の形態の1あるいは3のシステムにおいて、公開鍵PkSP－A，PkSP－Bを用いて暗号化される、クライアントCからサービスプロバイダSP－A，SP－Bへの情報の配送を利用して、クライアントCに認証代行サーバSで復号化ができないような形での認証情報を要求し、この認証情報を認証代行サーバSからサービスプロバイダSP－A，SP－Bへ転送して、サービスプロバイダSP－A，SP－Bでクライアント認証を行うものである。

【0060】図5において、A，BはそれぞれサービスプロバイダSP－A，SP－Bに対応するクライアントCの認証情報である。認証代行サーバSは、暗号用公開鍵PkSP－A，PkSP－BをクライアントCに配送する際に、この公開鍵PkSP－A，PkSP－Bを使った認証情報A，Bの暗号化要求をクライアントCに対して行う。

【0061】クライアントCは、サービスプロバイダSP－Aへ送信すべき情報を公開鍵PkSP－Aを用いて暗号化する際に、公開鍵PkSP－Aを用いて認証情報（パスワード）Aを暗号化した、この暗号化された認証情報Aを実施の形態の1あるいは3で説明した他の情報と共に認証代行サーバSへ送信する。同様に、クライアントCは、サービスプロバイダSP－Bへ送信すべき情報を公開鍵PkSP－Bを用いて暗号化する際に、公開鍵PkSP－Bを用いて認証情報（パスワード）Bを暗号化し、この暗号化された認証情報Bを実施の形態の1あるいは3で説明した他の情報と共に認証代行サーバSへ送信する。

【0062】サービスプロバイダSP－A，SP－Bは、クライアントCから送信され認証代行サーバSによって転送された情報を受け取り、この情報を暗号用秘密鍵SkSP－A，SkSP－Bを用いて復号化して、認証情報A，Bを取得する。そして、サービスプロバイダSP－A，SP－Bは、認証情報A，Bを基にクライアントCの認証を行う。

【0063】こうして、認証代行サーバSがクライアントCになりすますことを防ぐことができ、前記問題点2を解決することができる。また、認証代行サーバSが自身の秘密情報SkPでクライアント認証を受けたとしても、サービスプロバイダSP－A，SP－Bは、クライアントCの直接認証が可能で、かつ認証代行サーバSがクライアントCになりすますことを防ぐ手段を有していることになり、認証代行サーバSの責任を軽減させることが可能となる（前記問題点3の解決）。

【0064】認証代行サーバSを用いる利点の一つは、クライアントCで管理する秘密情報の数を減少させることであるから、本実施の形態での認証情報A，Bは認証代行サーバSで管理しているものと比べて簡易なものと

することが一般的となる。例えば、認証代行サーバＳは、秘密情報ＳｋＵ－Ａ，ＳｋＵ－ＢあるいはＳｋＰを利用したクライアント認証処理を行い、クライアントＣは、前記秘密情報よりも簡易なパスワードを認証情報として認証代行サーバＳに秘匿した形でサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂに送ることでクライアント認証を受ける。

【００６５】なお、毎回、同一のパスワードを転送する場合には、認証代行サーバＳによるリプレイ攻撃が可能になるため、シリアル値や時刻情報、あるいは実施の形態の３で説明したセッションキーと認証情報とを組み合わせて転送することも有効である。

【００６６】［実施の形態の６］図６は本発明の第６の実施の形態となる認証代行サーバＳの構成を示すブロック図である。図６に示す認証代行サーバＳは、実施の形態の１～５の認証代行サービスシステムを実現するものである。認証代行サーバＳは、少なくともクライアントＣの認証機能、及び暗号用公開鍵配送機能を持ち、実施の形態の３以外の場合には暗号用公開鍵証明書機能機能を持つ。

【００６７】なお、認証代行サーバＳがクライアントＣに代わってサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂからクライアント認証を受ける処理を従来技術２の方式で行う場合には、ＳｋＰ記憶器１０及びＣｅｒｔＰ記憶器１１は不要であり、従来技術３の方式で行う場合には、ＳｋＵ－Ａ記憶器８及びＣｅｒｔＵ－Ａ記憶器９は不要である。

【００６８】ＳｋＵ－Ｐ記憶器１は、認証代行サーバＳとクライアントＣ間の認証に用いるための秘密情報ＳｋＵ－Ｐを記憶し、ＣｅｒｔＵ－Ｐ記憶器２は、秘密情報ＳｋＵ－Ｐに対応した証明書ＣｅｒｔＵ－Ｐを記憶している。秘密情報ＳｋＵ－Ｐと証明書ＣｅｒｔＵ－Ｐとは、各クライアントＣ毎に記憶されている。

【００６９】ＳｋＵ－Ｐ検証器３は、クライアントＣから送信され送受信装置１４で受信された秘密情報ＳｋＵ－Ｐ、証明書ＣｅｒｔＵ－Ｐ、あるいは秘密情報ＳｋＵ－Ｐと証明書ＣｅｒｔＵ－Ｐとを基に、ＳｋＵ－Ｐ記憶器１及びＣｅｒｔＵ－Ｐ記憶器２を参照して、クライアントＣの認証を行う。ＳｋＵ－Ｐ検証器３は、一般には各クライアントＣの識別番号とそれぞれの秘密情報ＳｋＵ－Ｐの対応表を参照することで、クライアントＣの認証を行う。

【００７０】ＳＰ－Ａ公開鍵記憶器４は、暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂ（ＰｋＵ’－Ａ，ＰｋＵ’－Ｂ）を記憶し、ＳＰ－Ａ公開鍵証明書ＣＲＬ記憶器５は、この暗号用公開鍵に対応する公開鍵証明書ＣｅｒｔＳＰ－Ａ，ＣｅｒｔＳＰ－Ｂ（ＣｅｒｔＵ’－Ａ，ＣｅｒｔＵ’－Ｂ）のＣＲＬを記憶し、ＳＰ－Ａ上位認証局公開鍵証明書記憶器６は、上位認証局の公開鍵証明書を記憶している。暗号用公開鍵とＣＲＬと上位認証局の公開鍵証明書とは、各サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ毎に記憶されている。

【００７１】ＳＰ公開鍵証明書検証器７は、ＳＰ－Ａ公開鍵記憶器４、ＳＰ－Ａ公開鍵証明書ＣＲＬ記憶器５及びＳＰ－Ａ上位認証局公開鍵証明書記憶器６を参照して、暗号用公開鍵の検証を行う。なお、図６では図示していないが、実際には、ＣＲＬを取得する手段と、上位認証局公開鍵証明書を取得する手段が別途必要となる。

【００７２】ＳｋＵ－Ａ記憶器８は、秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂを記憶し、ＣｅｒｔＵ－Ａ記憶器９は、秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂに対応した証明書ＣｅｒｔＵ－Ａ，ＣｅｒｔＵ－Ｂを記憶している。秘密情報ＳｋＵ－Ａ，ＳｋＵ－Ｂと証明書ＣｅｒｔＵ－Ａ，ＣｅｒｔＵ－Ｂとは、各サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ毎及び各クライアントＣ毎に記憶されている。

【００７３】ＳｋＰ記憶器１０は、サーバＳ自身の秘密情報ＳｋＰを記憶し、ＣｅｒｔＰ記憶器１１は、秘密情報ＳｋＰに対応した証明書ＣｅｒｔＰを記憶している。署名生成器１２は、所定の通信文を秘密情報ＳｋＵ－Ａ，ＳｋＵ－ＢあるいはＳｋＰを用いて暗号化した署名を生成し、この署名を送受信装置１４を介してサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへ送信する。場合によっては、署名生成器１２は、前記署名と共に証明書ＣｅｒｔＵ－Ａ，ＣｅｒｔＵ－ＢあるいはＣｅｒｔＰをサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂへ送信する。

【００７４】代行処理部１３は、実施の形態の１～５で説明した処理以外の代行処理を必要に応じて行う。送受信装置１４は、ネットワークを介してクライアントＣ及びサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂと接続され、クライアントＣ及びサービスプロバイダＳＰ－Ａ，ＳＰ－Ｂとの間で情報の送受信を行う。

【００７５】なお、本実施の形態では、クライアント認証として公開鍵暗号を利用した認証方式によるものを想定しているが、認証方式によっては署名生成器１２、ＳｋＵ－Ｐ検証器３、及び証明書Ｃｅｒｔ類の記憶器５，６，９，１１は不必要になる。例えば、パスワード認証では証明書は必要がなく、また署名生成器１２も必要ない。

【００７６】以上のような認証代行サーバＳは、インターネット上などネットワーク上のサーバ、企業内ＬＡＮや家庭内ＬＡＮからインターネットなど広域ネットワークへのゲートウェイとして設置が可能であり、例えば、ワークステーション、パーソナルコンピュータ、ルータ、ターミナルアダプタなどの上でのソフトウェア、ハードウェア及び周辺機器として実現される。

【００７７】［実施の形態の７］図７は本発明の第７の実施の形態となるクライアントＣの構成を示すブロック図である。図７に示すクライアントＣは、実施の形態の１～５の認証代行サービスシステムを実現するものである。クライアントＣは、少なくとも暗号用公開鍵受信機

能、暗号用公開鍵による暗号化機能を持ち、実施の形態の２の場合にはクライアント暗号用秘密鍵による復号化機能、実施の形態の３の場合にはセッションキー生成／送信機能及びセッションキーによる暗号化／復号化機能、実施の形態の４の場合には暗号用公開鍵証明書検証機能を持つ。

【００７８】つまり、実施の形態の２以外の場合には、ＳｋＵ’－Ａ記憶器２６及び復号器２７は不要であり、実施の形態の３以外の場合には、ＳＳｋ生成器２８、ＳＳｋ一時記憶器２９、ＳｄＳＳＫ生成器３０及び暗号化／復号化器３１は不要であり、実施の形態の４以外の場合には、ＳＰ公開鍵証明書ＣＲＬ記憶器３２、ＳＰ上位認証局公開鍵証明書記憶器３３及びＳＰ公開鍵証明書検証器３４は不要である。

【００７９】ＳｋＵ－Ｐ記憶器２１は、認証代行サーバＳと自クライアントＣ間の認証に用いるための秘密情報ＳｋＵ－Ｐを記憶し、ＣｅｒｔＵ－Ｐ記憶器２２は、秘密情報ＳｋＵ－Ｐに対応した証明書ＣｅｒｔＵ－Ｐを記憶している。署名生成器２３は、所定の通信文を秘密情報ＳｋＵ－Ｐを用いて暗号化した署名を生成し、この署名を送受信装置３６を介して認証代行サーバＳへ送信する。場合によっては、署名生成器２３は、前記署名と共に証明書ＣｅｒｔＵ－Ｐを認証代行サーバＳへ送信する。

【００８０】ＳＰ公開鍵一時記憶器２４は、認証代行サーバＳから送信され送受信装置３６で受信された暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂを記憶している。暗号化器２５は、この暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂを用いて情報の暗号化を行い、暗号化された情報を送受信装置３６を介して認証代行サーバＳへ送信する。

【００８１】ＳｋＵ’－Ａ記憶器２６は、暗号用秘密鍵ＳｋＵ’－Ａ，ＳｋＵ’－Ｂを記憶している。この暗号用秘密鍵は、各サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ毎に記憶されている。復号器２７は、認証代行サーバＳから送信され送受信装置３６で受信された情報を暗号用秘密鍵ＳｋＵ’－Ａ，ＳｋＵ’－Ｂを用いて復号化する。

【００８２】ＳＳｋ生成器２８は、暗号通信用セッションキーＳＳｋＡ，ＳＳｋＢを生成し、ＳＳｋ一時記憶器２９は、この暗号通信用セッションキーＳＳｋＡ，ＳＳｋＢを記憶する。ＳｄＳＳＫ生成器３０は、セッションキーＳＳｋＡ，ＳＳｋＢの元となるデータＳｄＳＳＫＡ，ＳｄＳＳｋＢを生成する。

【００８３】暗号化／復号化器３１は、送信すべき情報をセッションキーＳＳｋＡ，ＳＳｋＢを用いて暗号化し、暗号化された情報を送受信装置３６を介して認証代行サーバＳへ送信する。また、暗号化／復号化器３１は、認証代行サーバＳから送信され送受信装置３６で受信された、暗号化された情報をセッションキーＳＳｋＡ，ＳＳｋＢを用いて復号化する。

【００８４】ＳＰ公開鍵証明書ＣＲＬ記憶器３２は、暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂに対応する公開鍵証明書ＣｅｒｔＳＰ－Ａ，ＣｅｒｔＳＰ－ＢのＣＲＬを記憶し、ＳＰ上位認証局公開鍵証明書記憶器３３は、上位認証局の公開鍵証明書を記憶している。ＣＲＬと上位認証局の公開鍵証明書とは、各サービスプロバイダＳＰ－Ａ，ＳＰ－Ｂ毎に記憶されている。

【００８５】ＳＰ公開鍵証明書検証器３４は、ＳＰ公開鍵証明書ＣＲＬ記憶器３２及びＳＰ上位認証局公開鍵証明書記憶器３３を参照して、認証代行サーバＳから送信され送受信装置３６で受信された暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂの検証を行う。なお、図７では図示していないが、実際には、ＣＲＬを取得する手段と、上位認証局公開鍵証明書を取得する手段が別途必要となる。

【００８６】入出力装置３５は、クライアントＣの利用者からの指示が入力されると、この指示をクライアントＣ内の各構成に出力すると共に、利用者に対して情報を出力する。送受信装置３６は、ネットワークを介して認証代行サーバＳと接続され、認証代行サーバＳとの間で情報の送受信を行う。

【００８７】なお、本実施の形態においても、認証代行サーバＳに対するクライアント認証機能は公開鍵暗号方式を想定しているが、認証方式によっては不必要になる回路が存在する。以上のようなクライアント装置Ｃは、パーソナルコンピュータ上のソフトウェアとして実現されるまた、一部若しくは全部の機能をスマートカード（ＩＣカード）などの安全なデバイス上で実現することも可能である。

【００８８】例えば、ＳｋＵ－Ｐ記憶器２１、ＣｅｒｔＵ－Ｐ記憶器２２及び署名生成器２３の機能をスマートカードに持たせ、残りの機能をスマートカードのリーダ／ライタ機能を備えたコンピュータ、電話機あるいはセットトップボックス等の処理装置に持たせることが可能であり、ＳｋＵ－Ｐ記憶器２１、ＣｅｒｔＵ－Ｐ記憶器２２及び署名生成器２３の機能と共にＳＰ公開鍵一時記憶器２４及び暗号化器２５の機能をスマートカードに持たせ、残りの機能を処理装置に持たせることも可能である。

【００８９】［実施の形態の８］図８、図９は本発明の第８の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。本実施の形態の認証代行サービスシステムは、実施の形態の５で説明したシステムをネットワークデビット決済用サーバ管理型ウォレットに適用したものである。

【００９０】ここで、ネットワークデビット決済の方式としては、ＳＥＴ（Online PIN Extensionを含む）あるいはＳＥＣＥを想定している。ネットワークデビット決済では、利用者、加盟店、金融機関ゲートウェイの３者

間での取引となるが、サーバ管理型ウォレットは、利用者のクライアントソフトへの処理負担を軽減するため、一般にネットワーク上に設置したサーバ上で動作するソフトである。現在、発表されているサーバ管理型ウォレットは、従来技術２に相当し、利用者が入力した銀行口座の暗証番号（ＰＩＮ）をサーバウォレットの動作するサーバで見ることができてしまう。利用者とサーバ管理型ウォレット間で暗号化したとしても、加盟店に送信する電文を作成するためには、一度復号化することになる。

【００９１】そこで、実施の形態の５で説明したシステムをネットワークデビット決済用サーバ管理型ウォレットに適用する。以下、本実施の形態のシステムの動作を図８、図９を用いて説明する。図８、図９において、ＰＧＷは銀行サーバ（サービスプロバイダ）、Ｍは加盟店、ＳＷはサーバウォレット（認証代行サーバ装置）、ＡＳは認証サーバ（クライアントＣと認証代行サーバ間の認証用）である。

【００９２】まず、図８に示すように、利用者がＩＣカードをクライアントＣに挿入して、クライアントＣの支払いボタンを押すと、加盟店Ｍから取引開始を示すイニシエーションがクライアントＣに送られる。続いて、利用者がカードパスワードを入力すると、認証サーバＡＳによってＩＣカードの認証が行われる。認証後、クライアントＣは、認証サーバＡＳに対してサービスログインを要求する。これにより、サービスが起動する。

【００９３】サービス起動後、サーバウォレットＳＷから利用者の口座を問い合わせるメニューが送られる。利用者は、クライアントＣを操作して所望の口座を指定する。利用者の口座を指定する情報がサーバウォレットＳＷに送られると、サーバウォレットＳＷは、銀行サーバＰＧＷとの間で所定の初期化処理を行う。

【００９４】次に、図９に示すように、サーバウォレットＳＷは、口座情報とＰＧＷ公開鍵（暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂに相当）とその他の情報（ＳＥＴ／ＳＥＣＥではＰＩＨｅａｄ）とをクライアントＣへ送信する。利用者は、ＰＩＮ（暗証番号、すなわち実施の形態の５の認証情報Ａ，Ｂに相当）をクライアントＣに入力する。ここで、ＳＥＴ／ＳＥＣＥでは、ＰＡＮＤａｔａと呼ばれる領域に、ＰＩＮあるいはＰＩＮのデータフォーマットを変換したものが含まれるため、これをクライアントＣにおいて組み立てる。

【００９５】そして、ＰＩＮ情報は、サービスプロバイダである銀行サーバＰＧＷにのみ通知し、サーバウォレットＳＷに対しては秘匿するために、クライアントＣにおいてＰＩＮ関連暗号データＨ（ＰＩＨｅａｄ＋ＰＡＮＤａｔａ）、Ｈ（ＰＡＮＤａｔａ）、Ｅ（ＰｋＰＧＷ，ＰＡＮＤａｔａ＋Ｋ）を計算する。ここでのＨ（）はハッシュ演算を示し、Ｅ（）はＲＳＡ演算を示す。こうして、ＰＧＷ公開鍵で暗号化されたＰＩＮ情報が銀行サーバＰＧＷに送られる。

【００９６】サーバウォレットＳＷから加盟店Ｍへの電文については、通常のクライアントＣからの電文、あるいは従来のサーバ管理型ウォレットからの電文フォーマットと合わせることで加盟店Ｍ、及び銀行サーバＳＷは従来どおりの機能のままで良い。

【００９７】これにより、銀行口座ＰＩＮはサーバウォレット事業者では解読困難となり、銀行口座ＰＩＮが漏洩するリスクを減少させることができる。また、金融機関が利用者をＰＩＮによって直接認証する手段をもつことにより、不正などが発生した場合の金融機関、サーバウォレット事業者、利用者間の責任所在の明確化が容易になる。なお、本実施の形態では、認証代行サーバを利用しない場合のクライアントと加盟店、加盟店と銀行サーバ間の電文には変更を加えないことが可能になっている。

【００９８】また、本実施の形態では、利用者にはスマートカードを配布し、クライアントとサーバウォレット事業者サーバ間の相互認証に利用することを想定している。ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）サーバ認証、あるいは、クライアント認証書をハードディスク上に格納した形態でのＳＳＬ相互認証を用いても構わない。しかし、一般に偽造が困難なスマートカードを利用することにより、仮に銀行口座ＰＩＮが利用者の管理ミスで他人に漏洩した場合にも、スマートカードのコピーや盗難が無い限りには、なりすまして決済を行われてしまうリスクは少なくなる。また、本発明のクライアントＣに相当するものとして上記スマートカードを利用した場合には、ＰＩＮ関連の処理のほとんどをスマートカード内で実行することにより、端末の共同利用などを考えた場合に、より安全性を向上させることが可能である。

【００９９】［実施の形態９］図１０は本発明の第９の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。本実施の形態の認証代行サービスシステムは、実施の形態の５で説明したシステムをネットワークデビット決済におけるサーバ管理型ウォレットの顧客証明書取得に適用したものである。

【０１００】なお、図１０では、クライアントＣとサーバウォレットＳＷ間の認証などシーケンス前半部分については、実施の形態の８と基本的に同一なため省略する。ＳＥＣＥなどにおいては、顧客証明書を顧客認証局に申請する以前に金融機関などから顧客特定暗証番号を郵送などにより入手しておく。これを顧客認証局への申請時に申請書内に記述し、顧客認証局はこの正当性を審査項目の一つとする。つまり、顧客認証局は、この顧客特定暗証番号により顧客の認証を行っていることになる（もちろん、この番号のみで認証しているわけではなく、申請書の記述内容のチェックなども併せて行う）。

【０１０１】従来のサーバ管理型ウォレットでは、実施の形態の８と同様に顧客特定暗証番号のサーバウォレット事業者への漏洩の問題がある。例えば、サーバウォレ

ット事業者の運用者がこれを盗聴し、顧客になりすました場合、顧客秘密鍵、及び対応する証明書の更新がなされ、なりすましてデビット決済を実行される恐れがある。

【０１０２】そこで、実施の形態の５で説明したシステムをネットワークデビット決済用サーバ管理型ウォレットに適用する。以下、本実施の形態のシステムの動作を図１０を用いて説明する。図１０において、ＣＣＡは顧客認証局である。まず、サーバウォレットＳＷは、申請書を顧客認証局ＣＣＡに要求して取得する。そして、サーバウォレットＳＷは、この申請書と共にＣＣＡ公開鍵（暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂに相当）をクライアントＣへ送信する。

【０１０３】利用者は、顧客特定暗証番号をクライアントＣに入力する。クライアントＣは、この顧客特定暗証番号をＣＣＡ公開鍵を用いて暗号化し、暗号化された情報をサーバウォレットＳＷへ送信する。サーバウォレットＳＷは、クライアントＣからの情報に顧客署名を付与した上で、顧客認証局ＣＣＡへ転送する。

【０１０４】顧客認証局ＣＣＡは、サーバウォレットＳＷから受け取った暗号化された情報をＣＣＡ秘密鍵で復号化して、顧客特定暗証番号を取得し、この顧客特定暗証番号を基に利用者の認証を行う。認証後、顧客認証局ＣＣＡは、証明書をサーバウォレットＳＷへ送信する。

【０１０５】以上のように、顧客特定暗証番号を暗号化して送信するため、サーバウォレット事業者での解読は困難になる。サーバウォレット事業者によるリプレイ攻撃を防ぐためには、顧客特定暗証番号に加えてシリアル番号など申請の度に異なる値を暗号化対象に含めることが望ましい。なお、本実施の形態の場合は、平成１１年９月現在公開されているＳＥＣＥ仕様における顧客認証局ＣＣＡの機能に加えて、顧客認証局暗号化用秘密鍵による顧客特定暗証番号の復号化機能が顧客認証局ＣＣＡに新たに必要になる。

【０１０６】［実施の形態の１０］図１１、図１２は本発明の第１０の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。本実施の形態の認証代行サービスシステムは、実施の形態の３で説明したシステムをＳＳＬ認証の認証代行サーバとして適用したものである。本実施の形態は、ＳＳＬ相互認証を行うものであり、暗号化アルゴリズムはＲＳＡを想定している。

【０１０７】クライアントとＳＳＬサーバの間で、従来のＳＳＬ認証を行う場合、クライアントには利用者の証明書・秘密鍵などの秘密情報が必要となる。前述の通り、利用者の秘密情報管理にはコスト・リスク等が伴うことが多いので、利用者の秘密情報をできるだけ少なくするために、認証代行サーバを利用するとする。ところが、全てのＳＳＬ認証を認証代行サーバで行わせるとなると、ＳＳＬの暗号化情報全てを、クライアントの代わりに認証代行サーバーで作成することになるので、ＳＳＬサーバとクライアント間の共通鍵を認証代行サーバで作成することが可能となる。これでは、認証代行サーバーにすべての秘密情報が漏れてしまう。

【０１０８】そこで、実施の形態の３を適用すると、ＳＳＬサーバとクライアント間で持つ、秘密情報の元となるプリマスターシークレット及びマスターシークレットの生成についてはクライアントで行わせ、プリマスターシークレットについては認証代行サーバで見ることができないように、通信時にはＳＳＬサーバの公開鍵で暗号化し、認証代行サーバに転送する。また、ＳＳＬサーバから要求されるクライアントの署名については、そのダイジェストをクライアントで作成し、認証代行サーバに転送し、認証代行サーバが利用者の秘密鍵で署名を施す。こうすることにより、認証代行サーバに利用者の秘密情報が漏れることなく、ＳＳＬ認証が可能となる。

【０１０９】以下、本実施の形態のシステムの動作を図１１、図１２を用いて説明する。まず、図１１に示すように、利用者がＩＣカードをクライアントＣに挿入し、カードパスワードを入力するとと、認証代行サーバＳによってＩＣカードの認証が行われる。認証後、クライアントＣは、認証代行サーバＳに対してサービスログインを要求する。これにより、サービスが起動する。

【０１１０】サービス起動後、認証代行サーバＳは、ＳＳＬサーバとの間で所定の初期化処理を行う。次に、図１２に示すように、認証代行サーバＳは、クライアントＣに対してクライアントキー（Ｃｌｉｅｎｔ Ｋｅｙ）を要求すると共に、サーバ公開鍵（暗号用公開鍵ＰｋＳＰ－Ａ，ＰｋＳＰ－Ｂに相当）をクライアントＣへ送信する。

【０１１１】クライアントＣは、プリマスターシークレット（データＳｄＳＳＫＡ，ＳｄＳＳＫＢに相当）を生成して、このプリマスターシークレットをサーバ公開鍵を用いて暗号化し、暗号化された情報を認証代行サーバＳへ送信する。こうして、サーバ公開鍵で暗号化されたプリマスターシークレットがＳＳＬサーバに送られる。さらに、クライアントＣは、プリマスターシークレットを基にマスターシークレットを生成して、このマスターシークレットに対してハッシュ演算を行い、このハッシュ演算を行った情報を認証代行サーバＳへ送信する。

【０１１２】以上のように、ＳＳＬ認証におけるほとんどの部分を認証代行サーバＳで行うことができるが、認証代行サーバＳに対して利用者が秘密にしておきたい部分であるプリマスターシークレット、マスターシークレットを生成する部分については、認証代行サーバＳから必要情報を与えることにより、クライアントＣで生成できる。

【０１１３】それ以外の部分については、認証代行サーバＳがＳＳＬサーバとの通信をすべて肩代わりする。図１２に示す「Ｆｉｎｉｓｈｅｄ」の部分をクライアントＣに送ることにより、双方向での暗号化通信（実施の形

態の３で説明したセッションキーを用いた暗号化通信に相当）が開始できる。その通信においては、認証代行サーバSは、ＳＳＬサーバとクライアントCで持っている共通鍵を知ることが無いので、通信内容が漏洩することなく、ＳＳＬサーバとクライアントＣ間で通信が可能である。

【０１１４】

【発明の効果】本発明によれば、認証代行サーバ装置が、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵をクライアント装置へ配送し、クライアント装置から受け取った暗号化された情報をサービスプロバイダ装置へ転送し、クライアント装置が、サービスプロバイダ装置へ送信すべき情報を暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信し、サービスプロバイダ装置が、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化することにより、認証代行サーバ装置には漏洩することなく、クライアント装置からサービスプロバイダ装置への情報転送を行うことができる。

【０１１５】また、認証代行サーバ装置が、所望のサービスに対応したサービスプロバイダ装置に対して、クライアント装置の暗号用公開鍵を配送し、サービスプロバイダ装置から受け取った暗号化された情報をクライアント装置へ転送し、サービスプロバイダ装置が、クライアント装置へ送信すべき情報を暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信し、クライアント装置が、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化することにより、認証代行サーバ装置には漏洩することなく、サービスプロバイダ装置からクライアント装置への情報転送を行うことができる。

【０１１６】また、認証代行サーバ装置が、所望のサービスに対応したサービスプロバイダ装置の暗号用公開鍵をクライアント装置へ配送し、クライアント装置から受け取った暗号化された情報をサービスプロバイダ装置へ転送し、サービスプロバイダ装置から受け取った暗号化された情報をクライアント装置へ転送し、クライアント装置が、サービスプロバイダ装置との間の暗号通信用セッションキーあるいはこのセッションキーの元となるデータを生成し、セッションキーあるいはデータを暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信した後、サービスプロバイダ装置へ送信すべき情報をセッションキーを用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信し、サービスプロバイダ装置が、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化してセッションキーを取得し、あるいは暗号用秘密鍵を用いた復号化によりデータを取得して、このデータからセッションキーを生成した後、クライアント装置へ送信すべき情報をセッションキーを用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信することにより、認証代行サーバ装置には漏洩することなく、クライアント装置とサービスプロバイダ装置間の双方向の情報転送を行うことができる。

【０１１７】また、認証代行サーバ装置が、暗号用公開鍵をクライアント装置へ配送する際に、暗号用公開鍵と共に暗号用公開鍵証明書を配送し、クライアント装置が、暗号用公開鍵を用いた暗号化を行う前に、認証代行サーバ装置から受け取った暗号用公開鍵証明書を基に暗号用公開鍵を検証するので、認証代行サーバ装置から配送される暗号用公開鍵を検証することができる。

【０１１８】また、クライアント装置が、暗号化を行う際に、自装置の認証情報を暗号用公開鍵を用いて暗号化し、この暗号化された情報を認証代行サーバ装置へ送信し、サービスプロバイダ装置が、復号化を行う際に、認証代行サーバ装置から受け取った暗号化された情報を暗号用秘密鍵を用いて復号化して認証情報を取得し、この認証情報を基にクライアント装置の認証を行うので、認証代行サーバ装置がクライアント装置になりすますことを防ぐことができ、さらに認証代行サーバ装置の責任を軽減させることが可能となる。

【図面の簡単な説明】

【図１】　本発明の第１の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。

【図２】　本発明の第２の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。

【図３】　本発明の第３の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。

【図４】　本発明の第４の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。

【図５】　本発明の第５の実施の形態となる認証代行サービスシステムの構成を示すブロック図である。

【図６】　本発明の第６の実施の形態となる認証代行サーバ装置の構成を示すブロック図である。

【図７】　本発明の第７の実施の形態となるクライアント装置の構成を示すブロック図である。

【図８】　本発明の第８の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。

【図９】　本発明の第８の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。

【図１０】　本発明の第９の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。

【図１１】　本発明の第１０の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。

【図１２】　本発明の第１０の実施の形態となる認証代行サービスシステムの動作を示すシーケンス図である。

【図１３】　従来のシステムの１例を示すブロック図である。

【図１４】　従来のシステムの他の例を示すブロック図である。

【図１５】　従来のシステムの他の例を示すブロック図である。

【図１６】　従来技術１の構成を示すブロック図である。

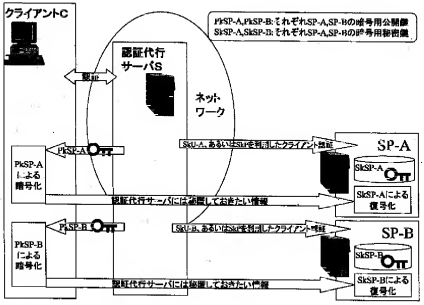
【図１７】　従来技術２の構成を示すブロック図である。

【図１８】　従来技術３の構成を示すブロック図である。

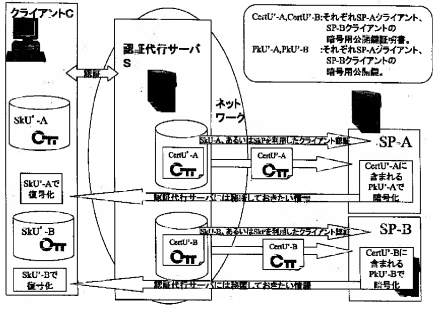
【符号の説明】

Ｃ…クライアント装置、Ｓ…認証代行サーバ装置、ＳＰ－Ａ、ＳＰ－Ｂ…サービスプロバイダ装置。

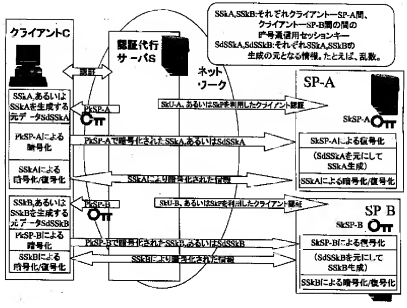
【図１】



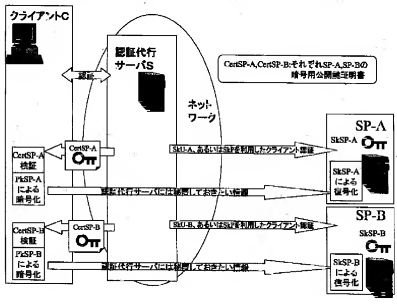
【図２】



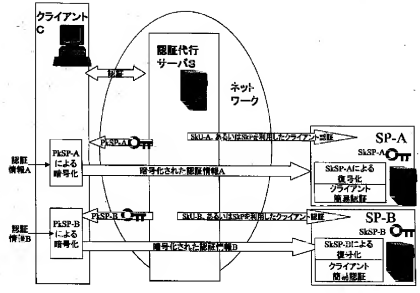
【図3】


SSkA,SSkB-それぞれクライアント—SP-A間、
クライアント—SP-B間の間の
PS号通信用セッションキー
SdSSkA,SdSSkB-それぞれSSkA,SSkBの
生成の元となる情報。たとえば、乱数。
クライアントC
認証代行
サーバS
認証
ネット
・ワーク
SP-A
SSkA,あるいは
SSkAを生成する
元データSdSSkA
PkSP-A
SkU-A, あるいはSkPを利用したクライアント認証
SkSP-A
PkSP-Aによる
暗号化
PkSP-Aで暗号化されたSSkA,あるいはSdSSkA
SkSP-Aによる復号化
(SdSSkAを元にして
SSkA生成)
SSkAによる暗号化/復号化
SSkAにより暗号化された情報
SSkA,あるいは
SSkBを生成する
元データSdSSkB
PkSP-B
SkU-B, あるいはSkPを利用したクライアント認証
SP B
SkSP-B
PkSP-Bによる
暗号化
PkSP-Bで暗号化されたSSkB,あるいはSdSSkB
SkSP-Bによる復号化
(SdSSkBを元にして
SSkB生成)
SSkBによる
暗号化/復号化
SSkBにより暗号化された情報

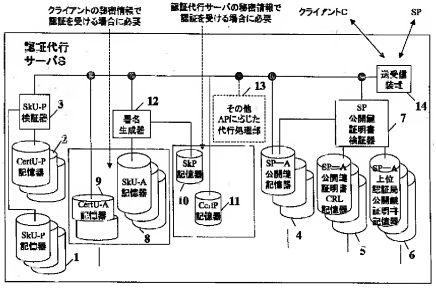
【図4】


クライアントC
認証代行
サーバS
CertSP-A,CertSP-B-それぞれSP-A,SP-Bの
暗号用公開鍵証明書
認証
ネット
・ワーク
SP-A
SkSP-A
CertSP-A
検証
CertSP-A
SkU-A, あるいはSkPを利用したクライアント認証
SkSP-A
による
復号化
PkSP-A
による
暗号化
認証代行サーバには秘匿しておきたい情報
CertSP-B
検証
CertSP-B
SkU-B, あるいはSkPを利用したクライアント認証
SP-B
SkSP-B
PkSP-B
による
暗号化
認証代行サーバには秘匿しておきたい情報
SkSP-B
による
復号化

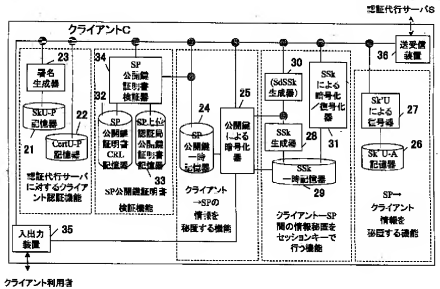
【図5】


クライアント
C
認証代行
サーバB
認証
ネット
ワーク
SkU-A、あるいはSkP-Aを利用したクライアント認証
SP-A
SkSP-A
PkSP-A
による
暗号化
暗号化された認証情報A
SkSP-Aによる
復号化
クライアント
署名認証
認証
情報A
PkSP-A
SkSP-B
SkU-B、あるいはSkP-Bを利用したクライアント認証
SP-B
SkSP-B
PkSP-B
による
暗号化
暗号化された認証情報B
SkSP-Bによる
復号化
クライアント
間の認証
認証
情報B

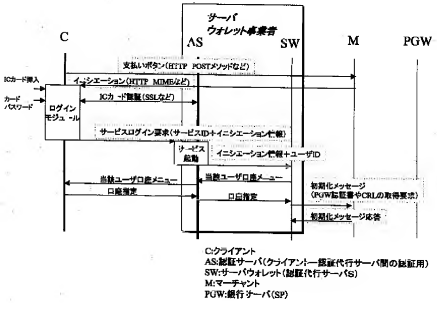
【図6】


クライアントの秘密情報で
認証を受ける場合に必要
認証代行サーバの秘密情報で認証を受ける場合に必要
クライアントに
SP
認証代行
サーバB
送受信
装置
14
SkU-P
検証器
3
12
署名
生成器
13
その他
APIにのじた
代行処理部
SP
公開鍵
証明書
検証器
7
2
CertU-P
記憶部
9
SkU-A
記憶部
SkP
記憶部
SP一A
公開鍵
記憶部
SP一A
公開鍵
証明書
CRL
記憶部
SP一A
上位
認証局
公開鍵
証明書
記憶部
CertU-A
記憶部
10
CoIP
記憶部
11
SkU-P
記憶部
1
8
4
5
6

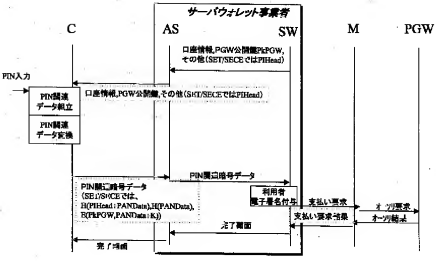
【図7】


認証代行サーバS
クライアントC
23
署名生成器
SKU-P記憶器
22
CertU-P記憶部
21
認証代行サーバに対するクライアント認証機能
34
SP公開鍵証明書検証器
32
SP公開鍵証明書CRL記憶部
SP公開鍵証明書検証機能
33
24
SP公開鍵一時記憶器
クライアント→SPの情報を秘匿する機能
25
公開鍵による暗号化器
30
(SdSSk生成器)
SSkによる暗号化/復号化器
SSk生成器
28
31
SSk一時記憶器
29
クライアント—SP間の情報秘匿をセッションキーで行う機能
36
送受信装置
SkU-Pによる復号器
27
SkU-A記憶部
26
SP→クライアント情報を秘匿する機能
入出力装置
35
クライアント利用者

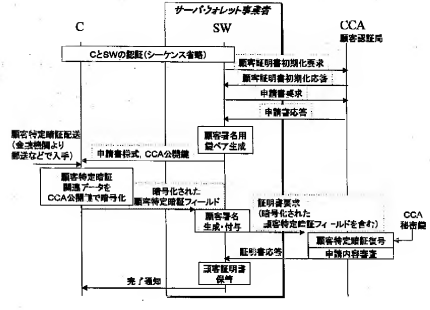
【図8】


サーバウォレット事業者
C
AS
SW
M
PGW
支払いボタン(HTTP POSTメソッドなど)
ICカード挿入
イニシエーション(HTTP MIMEなど)
カードパスワード
ICカード認証(SSLなど)
ログインモジュール
サービスログイン要求(サービスID+イニシエーション情報)
サービス起動
イニシエーション情報+ユーザID
当該ユーザ口座メニュー
当該ユーザ口座メニュー
口座指定
口座指定
初期化メッセージ(PGW加盟店申込URLの取得要求)
初期化メッセージ応答
C:クライアント
AS:認証サーバ(クライアント—認証代行サーバ間の認証用)
SW:サーバウォレット(認証代行サーバS)
M:マーチャント
PGW:銀行サーバ(SP)

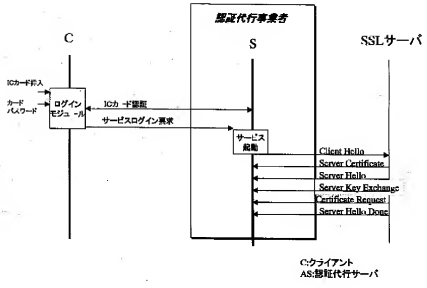
【図9】


サーバウォレット事業者
C
AS
SW
M
PGW
口座情報,PGW公開鍵,その他(SET/SECEではPIHead)
PIN入力
PIN関連データ転送
PIN関連データ変換
口座情報,PGW公開鍵,その他(SET/SECEではPIHead)
PIN関連暗号データ
(SET/SPCEでは、
H(PIHead+PANData),H(PANData),
E(PK:PGW,PANData+K))
利用者電子署名付与
支払い要求
支払い要求結果
オーソリ要求
オーソリ結果
完了画面
完了通知

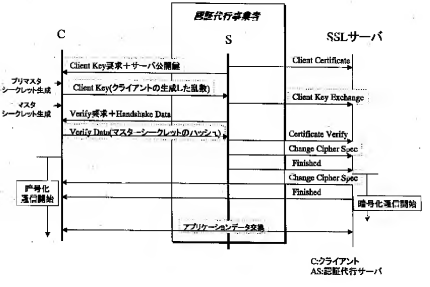
【図10】


サーバウォレット事業者
C
SW
CCA
顧客認証局
CとSWの認証(シーケンス省略)
顧客証明書初期化要求
顧客証明書初期化応答
申請書要求
申請書応答
顧客署名用鍵ペア生成
顧客特定暗証転送
(金流網とは別経路などで入手)
申請書様式、CCA公開鍵
顧客特定暗証関連データを
CCA公開鍵で暗号化
暗号化された顧客特定暗証フィールド
証明書要求
(暗号化された顧客特定暗証フィールドを含む)
CCA秘密鍵
顧客署名生成・付与
顧客特定暗証復号
証明書応答
申請内容審査
証明書発行・保存
完了通知

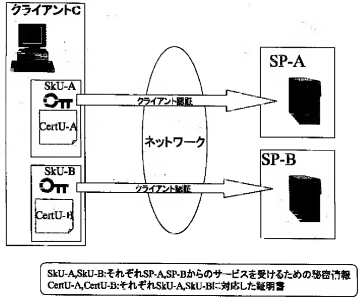
【図11】


認証代行事業者
C
S
SSLサーバ
ICカード挿入
カード
パスワード
ログイン
モジュール
ICカード認証
サービスログイン要求
サービス
開始
Client Hello
Server Certificate
Server Hello
Server Key Exchange
Certificate Request
Server Hello Done
C:クライアント
AS:認証代行サーバ

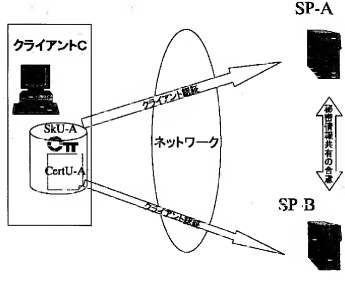
【図12】


認証代行事業者
C
S
SSLサーバ
Client Key要求＋サーバ公開鍵
Client Certificate
プリマスタ
シークレット生成
Client Key(クライアントの生成した乱数)
Client Key Exchange
マスタ
シークレット生成
Verify要求＋Handshake Data
Verify Data(マスターシークレットのハッシュ)
Certificate Verify
Change Cipher Spec
Finished
Change Cipher Spec
Finished
暗号化
通信開始
暗号化通信開始
アプリケーションデータ交換
C:クライアント
AS:認証代行サーバ

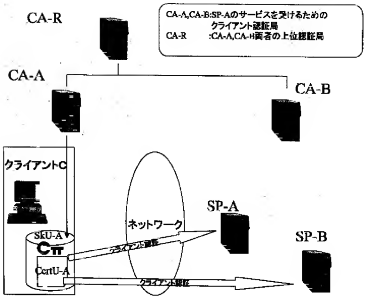
【図13】


クライアントC
SkU-A
CertU-A
SkU-B
CertU-B
クライアント暗証
クライアント暗証
ネットワーク
SP-A
SP-B
SkU-A,SkU-B:それぞれSP-A,SP-Bからのサービスを受けるための秘密情報
CertU-A,CertU-B:それぞれSkU-A,SkU-Bに対応した証明書

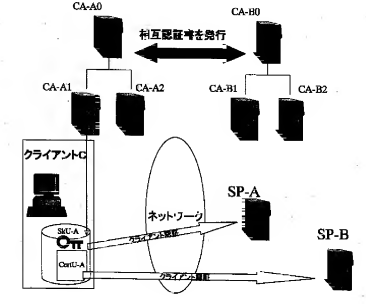
【図14】


SP-A
クライアントC
クライアント暗証
SkU-A
CertU-A
ネットワーク
秘密情報共有の仕組み
SP-B
クライアント暗証

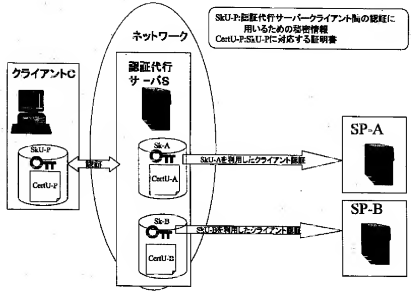
【図15】


CA-R
CA-A,CA-B:SP-Aのサービスを受けるための
クライアント認証局
CA-R :CA-A,CA-Bの発行者の上位認証局
CA-A
CA-B
クライアントC
SP-A
ネットワーク
SKU-A
SP-B
CertU-A
クライアント認証
クライアント認証

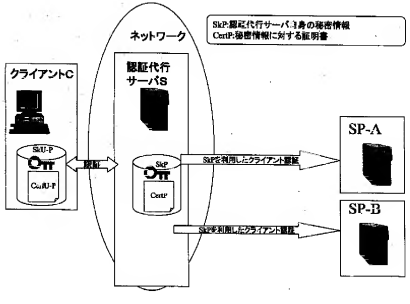
【図16】


CA-A0
CA-B0
相互認証書を発行
CA-A1
CA-A2
CA-B1
CA-B2
クライアントC
SP-A
ネットワーク
SKU-A
SP-B
CertU-A
クライアント認証
クライアント認証

【図17】



【図18】



フロントページの続き

(72)発明者　安田　仁
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

(72)発明者　山本　守孝
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

（72）発明者　桑田　晶彦
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
（72）発明者　今泉　法子
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
（72）発明者　嶋崎　剛
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

Ｆターム（参考）　5B085 AE13 AE23 AE29 BG07
5B089 GA19 GA21 JA32 JB22 KA17
KB13 KC58 KH30